Defence Research and Development Canada **Recherche et développement pour la défense Canada**

Harbour Siren

Technical Recommendations Report

Michael Abramson
Advanced Systems Management Group Ltd.

Prepared by:
Advanced Systems Management Group Ltd.
265 Carling Ave, Suite 630
Ottawa, ON K1T 4G3

Defence R&D Canada – Atlantic

Contract Report
DRDC Atlantic CR 2010-179
May 2011

Canada

This page intentionally left blank.

Harbour Siren

Technical Recommendations Report

Michael Abramson
Advanced Systems Management Group Ltd

Defence R&D Canada – Atlantic

Contract Report
DRDC Atlantic CR 2010-179
May 2011

Principal Author

Original signed by Michael Abramson

Michael Abramson

President, Advanced Systems Management Group Ltd

Approved by

Original signed by Francine Desharnais

Francine Desharnais

Head / Maritime Information and Combat Systems

Approved for release by

Original signed by Calvin Hyatt

Calvin Hyatt

DRP Chair

Abstract

This study was commissioned by Defence Research and Development Canada – Atlantic (DRDC Atlantic) as part of a project on Harbour Security that was funded by the Marine Security Coordination Fund of the Interdepartmental Marine Security Working Group (IMSWG). The document outlines a series of observations and technical recommendations resulting from a post Harbour Siren 2009 document review conducted by Advanced Systems Management Group Ltd. The review looked at the information, practices, standards, tools used during planning, execution and assessment of the Harbour Siren exercise, with the objective of the review being a set of recommendations and a near term road map for Emergency Management Interoperability (EMI) and Emergency Management System Interoperability (EMSI). The analysis provided recommendations related to: 1) the EMSI Capability Portfolio, focusing on the development/deployment voice and data interoperability capability; and 2) on Exercise Process Improvement, focusing on improving exercise planning, executions and assessment. The recommendations build on the Harbour Siren observations and provide strategies for the community to develop greater capability, flexibility, agility and adaptability in their ability to interoperate. Key areas include: A) shared community vision for voice and data communication; B) shared community understanding of requirements resulting from this shared vision; C) provision of shared situational/domain awareness; and D) enhancement of interagency collaboration.

Résumé

Cette étude a été commandée par Recherche et développement pour la défense Canada – Atlantique (RDDC Atlantique) dans le cadre d'un projet concernant la sécurité portuaire financé par le Fonds de coordination de la sûreté maritime du Groupe de travail interministériel sur la sûreté maritime (GTISM). Le document présente un ensemble d'observations et de recommandations techniques résultant d'un examen de documents connexes à l'exercice *Harbour Siren* 2009, qui a été effectué par *Advanced Systems Management Group Ltd*. L'examen a porté sur l'information, les pratiques, les normes et les outils utilisés durant la planification, l'exécution et l'évaluation de l'exercice *Harbour Siren*, dans le but de dégager un ensemble de recommandations et une feuille de route à court terme pour l'interopérabilité dans la gestion des urgences (IGU) et l'interopérabilité du système de gestion des urgences (ISGU). Cette analyse a permis de dégager des recommandations relativement : 1) au portefeuille de capacités de l'ISGU, axé sur le développement et la mise en œuvre d'une capacité d'interopérabilité voix-données; 2) à l'amélioration du processus des exercices, axée sur l'amélioration de la planification, de l'exécution et de l'évaluation des exercices. Les recommandations sont basées sur l'observation de l'exercice *Harbour Siren*, et elles fournissent à la communauté des stratégies pour développer une plus grande capacité, flexibilité, souplesse et adaptabilité en matière d'interopérabilité. Elles portent essentiellement sur les points suivants : A) perception commune, au sein de la communauté, pour les transmissions vocales et de données; B) compréhension commune des exigences découlant de cette perception; C) développement d'une connaissance commune de la situation/du domaine; D) renforcement de la collaboration interorganismes.

This page intentionally left blank.

Executive summary

Harbour Siren: Technical Recommendations Report

Michael Abramson; DRDC Atlantic CR 2010-179; Defence R&D Canada – Atlantic; May 2011.

Introduction: This study was commissioned by Defence Research and Development Canada – Atlantic (DRDC Atlantic) as part of a project on Harbour Security that was funded by the Marine Security Coordination Fund of the Interdepartmental Marine Security Working Group (IMSWG). The document outlines a series of observations and technical recommendations resulting from a post Harbour Siren 2009 document review conducted by Advanced Systems Management Group Ltd. The review looked at the information, practices, standards, tools used during planning, execution and assessment of the Harbour Siren exercise, with the objective of the review being a set of recommendations and a near term road map for Emergency Management Interoperability (EMI) and Emergency Management System Interoperability (EMSI).

Results: The analysis provided recommendations related to: 1) the EMSI Capability Portfolio, focusing on the development/deployment voice and data interoperability capability; and 2) on Exercise Process Improvement, focusing on improving exercise planning, executions and assessment. The recommendations build on the Harbour Siren observations and provide strategies for the community to develop greater capability, flexibility, agility and adaptability in their ability to interoperate. Key areas include: A) shared community vision for voice and data communication; B) shared community understanding of requirements resulting from this shared vision; C) provision of shared situational/domain awareness; and D) enhancement of interagency collaboration.

Significance: Gaps in information, operational and technical interoperability have been and continue to be a challenge for the emergency and public security communities. Emergency managers and government decision makers require access to relevant and accurate information in order to more effectively exercise their responsibilities. Improving the quality of information, and making that information "discoverable", "accessible", and "understandable" is one of the central pillars of Public Safety's mandates and the focus of a number of their Reports on Plans and Priorities over the last decade.

Future plans: The report includes near-term roadmap activities in the areas of business architecture, domain models, high-risk interoperability services and open standards development. Many of these recommendations are aimed at the R&D community, in support of the Emergency Management community. The recommendations should be useful to DRDC Centre for Security Science to develop and prioritize research projects in these areas.

The recommendations included in this report are those of the Contracting team. The DRDC recommendations were compiled from this and other Contractor Reports, and are published in the DRDC final report to IMSWG.

Sommaire

Harbour Siren: Technical Recommendations Report

Michael Abramson; DRDC Atlantic CR 2010-179; R & D pour la défense Canada – Atlantique; mai 2011.

Introduction : Cette étude a été commandée par Recherche et développement pour la défense Canada – Atlantique (RDDC Atlantique), dans le cadre d'un projet concernant la sécurité portuaire financé par le Fonds de coordination de la sûreté maritime du Groupe de travail interministériel sur la sûreté maritime (GTISM). Le document présente un ensemble d'observations et de recommandations techniques résultant d'un examen de documents connexes à l'exercice *Harbour Siren* 2009*,* qui a été effectué par *Advanced Systems Management Group Ltd*. L'examen a porté sur l'information, les pratiques, les normes et les outils utilisés durant la planification, l'exécution et l'évaluation de l'exercice *Harbour Siren*, dans le but de dégager un ensemble de recommandations et une feuille de route à court terme pour l'interopérabilité dans la gestion des urgences (IGU) et l'interopérabilité du système de gestion des urgences (ISGU).

Résultats : Cette analyse a permis de dégager des recommandations relativement : 1) au portefeuille de capacités de l'ISGU, axé sur le développement et la mise en œuvre d'une capacité d'interopérabilité voix-données; 2) à l'amélioration du processus des exercices, axée sur l'amélioration de la planification, de l'exécution et de l'évaluation des exercices. Les recommandations sont basées sur l'observation de l'exercice *Harbour Siren*, et elles fournissent à la communauté des stratégies pour développer une plus grande capacité, flexibilité, souplesse et adaptabilité en matière d'interopérabilité. Elles portent essentiellement sur les points suivants : A) perception commune, au sein de la communauté, pour les transmissions vocales et de données; B) compréhension commune des exigences découlant de cette perception; C) développement d'une connaissance commune de la situation/du domaine; D) renforcement de la collaboration interorganismes.

Importance : Des lacunes en matière d'information ainsi que d'interopérabilité technique et opérationnelle ont été et continuent d'être un défi pour les collectivités chargées de la gestion des urgences et de la sécurité publique. Les gestionnaires des mesures d'urgence et les décideurs gouvernementaux doivent avoir accès à de l'information pertinente et exacte pour assumer efficacement leurs responsabilités. Le fait d'améliorer la qualité de l'information et de rendre celle-ci « trouvable », « accessible » et « compréhensible » est l'un des principaux axes des mandats de Sécurité publique Canada, et il constitue le point central de bon nombre de ses rapports sur les plans et les priorités au cours des dix dernières années.

Plans futurs : Le rapport englobe des activités à court terme de la feuille de route dans les secteurs de l'architecture des activités, des modèles de domaines, des services d'interopérabilité à risque élevé et de l'élaboration de normes transparentes. Bon nombre de ces recommandations ciblent la collectivité de R & D, à l'appui de la collectivité de gestion des urgences. Ces recommandations devraient aider le Centre des sciences pour la sécurité de RDDC à élaborer des projets de recherche dans ces domaines et à les classer par ordre de priorité.

Les recommandations intégrées dans le rapport sont celles qui ont été formulées par le groupe contractuel. Les recommandations de RDDC ont été compilées à partir du présent rapport et d'autres rapports d'entrepreneurs, et elles sont publiées dans le rapport final de RDDC adressé au GTISM.

This page intentionally left blank.

Table of contents

List of figures

This page intentionally left blank.

1 Introduction

1.1 Scope

This document was prepared for Defence Research and Development Canada – Atlantic. The document outlines a series of observations and technical recommendations resulting from a post Harbour Siren 2009 document review conducted by Advanced Systems Management Group (ASMG) Ltd between January and March 2010. The review looked at the information, practices, standards, tools used during planning, execution and assessment of the Harbour Siren exercise, with the objective of the review being a set of recommendations and a near term road map for Emergency Management Interoperability (EMI) and Emergency Management System Interoperability (EMSI).

Gaps in information, operational and technical interoperability have been and continue to be a challenge for the emergency and public security communities. Emergency managers and government decision makers require access to relevant and accurate information in order to more effectively exercise their responsibilities. Improving the quality of information, and making that information "discoverable", "accessible", and "understandable" is one of the central pillars of Public Safety's mandates and the focus of a number of their Reports on Plans and Priorities over the last decade.

The challenges faced by the public safety community to develop and sustain operational interoperability mirror that of other diverse operational communities. One area of focus is enhancing the community's capacity to translate lessons learned during operations and exercises into enhanced community capability. DRDC Atlantic is seeking to support the EM community and provide a set of observations, recommendations and roadmap elements based in the Harbour Siren Exercise. This report represents one in a set of parallel efforts to do so.

1.2 Background

The Governments of Canada (GC) is committed to improving marine security in Canada's territorial waters and shore facilities; as stated in Canada's National Security Policy (NSP). Marine security, specifically port security, has been identified as one of the Government of Canada's top priorities. Exercise Harbour Siren was a full-scale marine safety and security management exercise. The exercise will involve representatives from a large number of stakeholders for maritime port operations, including participation from municipal, provincial, federal agencies and the private sector.

Multiple emergency management exercises and real-world events such as the Ice Storm and SARS have shown that improved situational (domain) awareness, and collaboration (e.g. Planning and Decision support are needed. This need was expressed by many participants in term of their difficulties maintaining situational awareness during the exercise. DRDC Atlantic is seeking to use the experiences of Harbour Siren to support recommendations to enhance the GC's ability to plan, execute and assess future operations and exercises and translate lessons learned into enhanced real-world capability.

In parallel, Public Safety Canada is developing an Emergency Management System Interoperability (EMSI) framework (EMSIF), which describes a set of practices and tools to enhance EMSI. The study is seeking to leverage these practices and tools as part of the study and the presentation of roadmap activities.

1.3 DRDC Contributions to Harbour Siren 09

The DRDC contribution to Harbour Siren is funded through the Interdepartmental Marine Security Working Group (IMSWG). DRDC's role is to support Public Safety Canada by measuring and assessing the community's ability to share and exploit information during the planning, response and recovering stages of an operation. DRDC'S role was to assess the effectiveness of the community's command and control, and information management capability during an operation that involved the three levels of government and private sector stakeholders; in specific, an emergency management and public security incident in the harbour domain.

The first phase of this IMSWG project was to map current information processes for a skeleton exercise scenario based on a ship on fire in the Halifax harbour. The scenario was selected to emphasize the grey areas for the in-harbour on-water response, in terms of roles and responsibilities for agencies involved at all 3 levels of government, and identify possible solutions to existing gaps. For this 1st phase, twelve agencies were interviewed and several DODAF views were modeled. The models illustrated the information and decision processes for the scenario (this work was performed by CAE, Consulting Group).

In parallel, a set of metrics were developed to support the assessment of the effectiveness of various community practices and systems:

- Command and Control (C2)
  - Authority (Lead Department/Agency)
  - Authority (Supporting Departments)
  - Doctrine
  - Organizational Structure
  - Personnel
  - Equipment
  - Communications
  - Interoperability
- Information Sharing
  - Situational Awareness at Lead Department Operations Center
  - External Communications

The metrics are intended to provide consistency in the assessment of observable criteria that are useful in determining the effectiveness of current capability and identify where S&T is required to augment that capability. Outputs from post exercise evaluations are seeking to determine if:

- The information capture, processing and dissemination practices and technologies provided quality information to the users, decision makers and stakeholders; where quality is based on the following criteria:

  - **Accurate**: semantics to accurately convey the perceived situation.

  - **Relevant**: information tailored to specific requirements of the mission, role, task or situation at hand.

  - **Timely**: information flow required to support key processes, including decision making.

  - **Usable**: information presented in a common, easily understood format.

  - **Complete**: information that provides all necessary (or available) information needed to make decisions.

  - **Brief**: information tailored to the level-of-detail required to make decisions and reduces data overload.

  - **Trustworthy**: information quality and content can be trusted by stakeholders, decision makers and users.

  - **Secure/protected**: Information is protected from inadvertent or Malicious Release or use.

- Are there identifiable gaps in the community's information sharing capability: Technology (networks, communications, platforms, information and/or applications); policy and procedures; roles and responsibilities; and/or practices for handling of sensitive information (private, confidential, classified) issues, etc.

- The importance of the community's informal processes and relationships in the sharing of situation, goals/objectives, needs or targets? What effect does this reliance have on overall (community level) situational awareness and operational performance? Are these informal processes linked to individuals or operating procedures? What might happen if these individuals are taken out of the loop (off-duty, retirement)?

The assessment of the exercise will result in the gathering of lessons learned and various observations. From this information, DRDC plans to prepare a series of capability recommendations for Public Safety and the S&T community. The recommendations will be incorporated into a near term roadmap that will specifically address priority needs and lessons learned. This study will provide some of the input to the development of the EMI roadmap.

1.4   Study Objectives

As illustrated in Figure 1-1, DRDC Atlantic is seeking to leverage the operational and technical lessons learned during the Harbour Siren Tabletop and interoperability exercises and provide element of a roadmap to enhance EMI/EMSI capability. More specifically, the study seeks to:

- Provide recommendations that would assist in the development roadmap for the enhancement of community EMSI in the maritime and harbour security domain:

- Identify risk areas and operational challenges that could be mitigated by additional research studies;

- Identify risk areas and operational challenges that could be mitigated by emerging technologies whose capabilities need to be ratified.

- Identify risk areas and operational challenges that could be mitigated by the development of open and/or community standards;

- Identify other capabilities that could be delivered by research establishments.

- Identify areas of current research that could be used to address EM and PS capability gaps.

- Provide recommendations that would focus resources community priorities; mitigate risk; and better manage the deployment of needed capability.

- Identify how the EMSIF could be leveraged to support these efforts.

- Provide recommendations that would improve the way interoperability exercises are planned, executed and evaluated – and ensure that lessons learned are incorporated into EMSI development portfolios.
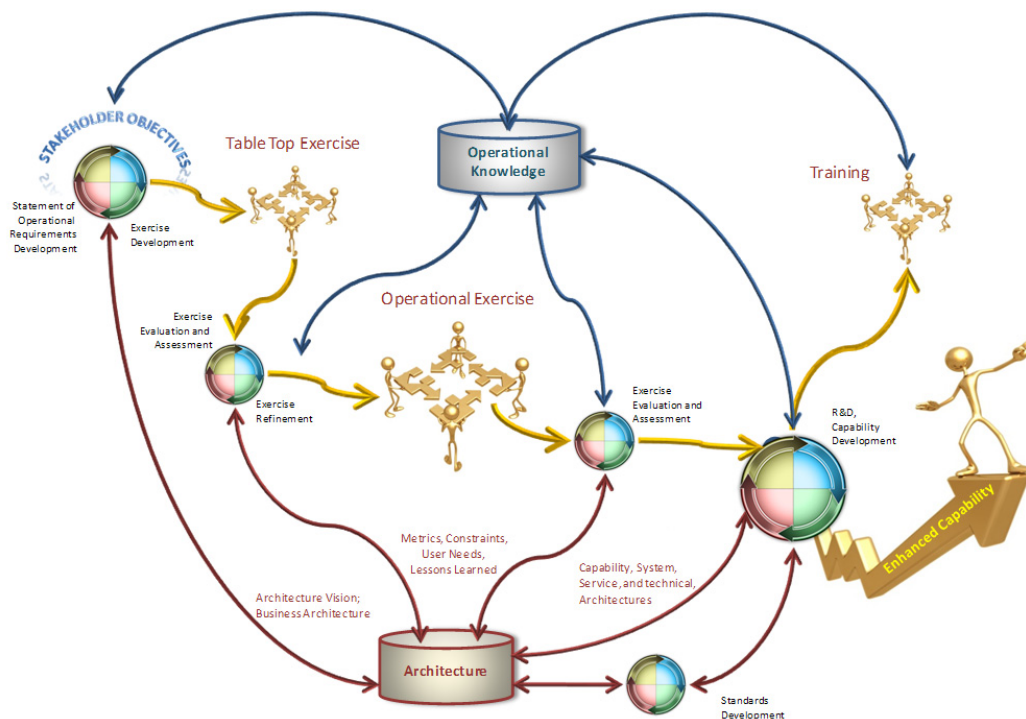
Figure 1: Leveraging Interoperability Exercises

This study is being conducted in parallel with other studies that are evaluating and assessing the capabilities of participating agencies and GC infrastructure. Observations by team members will be shared with other teams for further assessment and action.

1.5   Reviewed Documents

The following documents were reviewed during the course of this study.

1. Preliminary Report on Metrics Development for Inter-Agency Maritime Emergency Response Operations Harbour Siren 2009, Intellection Consulting

2. Harbour Siren Exercise: Evaluators Guide, October 2009

3. Harbour Siren Exercise: Exercise Design Team Guide, October 2009

4. Harbour Siren Exercise: Player Handbook, September 2009

5. Harbour Siren Exercise: After Action Report, Tabletop Exercise, December 2008

6. Harbour Siren Exercise: Major Scenario Event List (MSEL)

7. Harbour Safety and Security Process Mapping, CAE consulting

8. Inter-agency Harbour Security Model Update, January 2010

9. HTML of the Inter-agency Harbour Security Model Update

10. Public Safety's Reports on Planning and Priorities

11. 2009 Auditor General's Report

12. Emergency Management System Interoperability (EMSI) Frame Vision

13. Emergency Management System Interoperability (EMSI) Frame Overview

14. Emergency Management System Interoperability (EMSI) Frame Road Map

2   Observations

2.1   Overview

This study is based solely on a review of the documents produced during planning, execution and assessment of Harbour Siren 2009 and March 2009 Workshop. The authors did not directly observe or participate in the execution of HS 2009 exercise. Based on this review, the study offers the following observations.

The observations are provided from the context of the community as a whole and is solely intending to identify and prioritize roadmap activities that would provide the greatest benefit to the community over the near and mid terms.

2.2   HS 09 Observations

Annexes A and B provide observations resulting from a review of the documentation identified in section 1.3. The central theme for most of the observations identified below is the gaps in the information compiled during the planning, execution and assessment of the exercise that would assist in the performance of GAP (Practice / process), Training, information and technology) analysis and the development of S&T and capability roadmaps.

Developing the ability to interoperate with other jurisdictions, organizations, people and systems (technology) is a major undertaking, which challenges the most technically savvy agencies. There a many hurdles that cannot be overcome by a single organization or agency. It will be the community coming together and sharing the information about the strengths and weaknesses of their capabilities, and collaborating with an expanding community that will provide the needed solutions. The observations and recommendation in this report are intended to support this building of community and a common purpose in jointly addressing the challenges.

2.3   Emergency Management and Systems Interoperability General Observations

This section provides some general observations of the EMS community and some of the challenges they face. Most have been identified in the additional notes and comments in the observations above. Many are within the S&T community to address on behalf of the broader community.

3 Recommendations

Based on the observations contained in Annexes A and B, the following recommendations are being put forward. These recommendations are categorised as follows:

1. EMSI Capability Portfolio: focuses on the development/deployment voice and data interoperability capability; and

2. Exercise Process Improvement: focuses on improving exercise planning, executions and assessment.

In general the recommendations build on the HS observations (Annexes A and B) and provide strategies for the community to develop greater capability, flexibility, agility and adaptability in their ability to interoperate. Key areas include:

1. Shared community vision for voice and data communication.

2. Shared community understanding of requirements resulting from this shared vision;

3. Provision of shared situational/domain awareness; and

4. Enhancement of Interagency collaboration.

3.1 Maritime EMSI Capability Portfolio

A central focus of this study was to take the Lessons Learned (observations) and translate them into a series of recommendations for the enhancement of maritime/harbour EMSI capability. Annex C.1 contains the recommendations that focus on community level strategies and solutions.

3.2 Exercises and Training Process Improvement

Annex C.2 contains the recommendations related to the improvement of practices, processes, and tools for the planning, staging, execution and evaluation of interoperability exercises. The objective of the recommendations is to provide the government of Canada with the capacity to develop and stage tabletop and full exercise in a progressive and cost effective manner. The industry best practices being followed in the development of this recommendation includes the foundations of the Capability Maturity Model (CMM), which provides a methodology for the development and refinement of an organization's practices and process. The models typically describe a five-level evolutionary path of increasingly organized and systematically more mature processes. The initial CMM was developed for the software development process and is promoted by the Software Engineering Institute (SEI), a research and development centre sponsored by the U.S. Department of Defense (DoD). In recent years, similar concepts have been used to develop maturity models for a host of operational and technical processes. The five-levels of capability include:

- At the *initial* level, processes are disorganized, even chaotic. Success is likely to depend on individual efforts, and is not considered to be repeatable, because processes would not be sufficiently defined and documented to allow them to be replicated.

- At the *repeatable* level, basic project management techniques are established, and successes could be repeated, because the requisite processes would have been established, defined, and documented.

- At the *defined* level, an organization has developed its own standard process through greater attention to documentation, standardization, and integration.

- At the *managed* level, an organization monitors and controls its own processes through data collection and analysis.

- At the *optimized* level, processes are constantly being improved through monitoring feedback from current processes and introducing innovative processes to better serve the organization's particular needs.

The Community should be targeting a "DEFINED" level of capability in the planning, execution and assessment, of training and exercise events.

As the planning, preparation and development of EM and PS exercises are the purview of PS, specific recommendation on activities have not been provided; with two exceptions. It is recommended that DRDC develop:

- A domain model to support the capture of planning and execution data to support post exercise analysis and the identification of required S&T activities.

- Metric for the assessment of exercise capability and the identification of required S&T activities.

3.3   General Education

Based on the reviewed documents, experience with the broader public safety community and comments from the HS workshop (March 9th 2010), there are community elements that needed to be addressed. However these elements fall outside the task oriented roadmap provided in section 4.   Within the maritime/harbour security community, there are significant differences in participant and stakeholder appreciation   of the technical challenges involved in developing, deploying and sustaining interoperable information systems for interagency Situational Awareness (SA) or collaboration (Planning, resource Management, etc...).   It is a persistent challenge to present concepts, strategies and approaches that are meaningful to such a diverse community. More effort to educate the community it required.

Most of the recommendations in this report revolve around the development of a shared (community) understanding about the business needs, operational capabilities, and strategies for underpinning interoperability. In engineering terms – establish an agreed set of requirements:

- Description of the entities (organizations, infrastructure, resources, etc...) in the environment and the relationships between them;

- How things work (or don't work) today and how they are expected to work in the future;

- What are community members expectations for interoperable environment; and

- What are the obstacles, challenges and risks?

Based on this information, the community can develop a roadmap for a staged enhancement of capability. At present, this information or understanding is fragmented and difficult to come to terms with. It does not have general agreement and is not documented in a form that is easily understood. In a number of areas there appear to be as many opinions as there are stakeholders.

By their very nature, systems (human, mechanical, electronic, etc.) require a shared set of requirements (agreements/understandings/interface-definitions/language) to interoperate. There needs to be some agreement of objectives and approach. This does not appear in the public safety domain or security domains. However, there does appear to be a growing desire for improved situational awareness. But there again the opinions of what that means differ widely.

It is recommended that a broad program of education and training be established, where the community members (Harbour/Maritime Security) can access a knowledge base comprising: books and resource materials (whitepapers, models, standards, specifications, designs..., Open Source capabilities) espousing community strategies and approaches; workshop; mentoring and one-on-one resources. Not all stakeholders can absorb this information in the same manner and at the same rate – but each needs this knowledge to make the decisions requisite to the development of capabilities needed for system and organizational interoperability.

The roadmap elements in Section 4 outline discrete tasks to allow the community to start accumulating information for the knowledge base. The larger challenge is educating the community – and the success of this broader effort will depend on the community's willingness to learn and adapt to their shared responsibilities. These challenges are beyond the scope of one or more tasks and require broader discussion within the community.

4 Proposed Near-Term Roadmap Activities

4.1 Business Architecture

4.1.1 Architecture Vision

As illustrated in Figure 4-1, the first stage in the development of an architecture model (blueprint for the maritime/harbour security) is to define the vision or defining the scope, identifying the stakeholders, creating the Architecture Vision, and obtaining approvals.
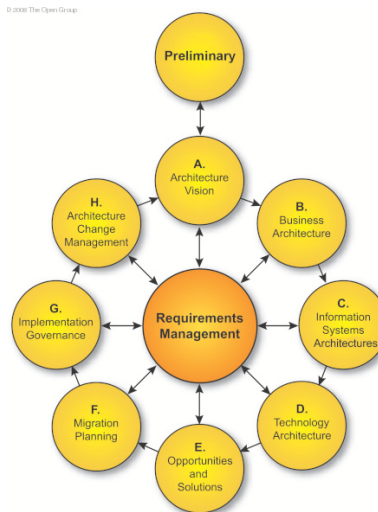
Figure 2: TOGAP ADM

One of the elements in the development of the vision is the identification of the architecture approaches to be adopted and how they are applied. For these elements, it is recommended that the community adopt the direction of the PS EMSIF architecture frameworks:

1. **TOGAF**: identifying the stages and activities involved in the development of enterprise, capability, system of systems and systems architectures.

2. **DODAF:** identifies the views, models and products to be developed during each stage of the architecture development. DODAF also provides the domain model for architecture views being developed.

3. **UPDM**: identifies the modelling profiles to be use to develop the architecture views and products in a consistent manner. Modelling to vendors are providing tools that support UPDM.

This direction will assist the community in several ways:

- The community will have common shared methods for describing and sharing their needs and capabilities vs. the myriad of threats, incidents and events to be addressed.

- The community will have a common set of artefacts that will simplify communication and information sharing;

- The community will have access to a range of off-the-shelf tools to support the definition and sharing of needs and capabilities before, during and after an incident or event.

This initial focus on architecture is based on the fundamentals of engineering and solving complex challenges:

- Understanding the problems is more than half the problem;

- Making sure we a addressing the right set of problems is the other half.

The solution is what results. The deployment of interoperable capability starts with the development of a maritime/harbour security vision[1]. Harbour Siren provides a lot of insight into the challenges, needs and current capability, but it does not document the whole story. It is recommended that the community initiate the preparation of a vision for maritime/harbour security (who, what, where, when, why and how) and document this as part of a business (/conceptual) architecture – available to all members of the community. As TOGAF recommends, this requires the completion of a vision stage (started by PS EMSIF) which addresses the following objectives:

- ensure that this evolution of the architecture development cycle (TOGAF tailored to community needs) has proper recognition and endorsement from the corporate management of the enterprise, and the support and commitment of the necessary line management

- define and organize an architecture development cycle within the overall context of the architecture framework;

- validate the business principles, business goals, and strategic business drivers of the organization and the enterprise architecture Key Performance Indicators (KPIs);

- define the scope of, and to identify and prioritize the components of, the Baseline Architecture effort;

- define the relevant stakeholders, and their concerns and objectives;

- define the key business requirements to be addressed in this architecture effort, and the constraints that must be dealt with;

- articulate an Architecture Vision and formalize the value proposition that demonstrates a response to those requirements and constraints;

- create a comprehensive plan that addresses scheduling, resourcing, financing, communication, risks, constraints, assumptions, and dependencies, in line with the capability management frameworks adopted by the enterprise;

- secure formal approval to proceed;

---

[1] Paraphrased from http://www.opengroup.org/architecture/togaf9-doc/arch/

- understand the impact on, and of, other enterprise architecture development cycles ongoing in parallel; and

- assure that all stakeholders have agreed to the objectives and possess a reasonable understanding of the challenges being addressed and the strategies being adopted.

This element of the roadmap represents a community-centred requirement and therefore has not specified tasking other than the general goals/objectives (above). The following sections identify activities that can be used to support these goals.

4.1.2 Maritime Situational Awareness (SA) / Domain Awareness (DA) Domain Models

At the core of maritime/harbour security is the ability of decision makers (at all levels) to gather, collate, aggregate and assess relevant information from a diverse set of sources; this is often referred to as a common operating picture (COP). This picture is then disseminated to supporting agencies, organizations, units and individual who in term collate, aggregate and action the information. The process of assessing the COP is what the community refers to as developing situational awareness. Lessons learned from multiple exercises and operations identify the decision makers often complained about a lack of situational awareness; Harbour Siren reported the same challenges. What is meant is that decision makers did not have access to the information needed to develop the awareness needed to make the most effective decisions.

A COP facilitates decision making and assists all participants to a multi-agency operation: plan, coordinate and execute assigned tasking. The COP underpins each agency's, or decision maker's ability to develop and maintain situational awareness: accurate perception and understanding of all the factors and conditions pertaining to the operational environment. The decision maker's perception of environmental conditions within a volume of time and space, understanding of relationships between each entity in the environment, and the projection of each entities status is critical to his/her effectiveness in this complex, dynamic environment: planning for, response to and recovery from an incident related to maritime or harbour security.

The COP can address a wide range of Information domains including:

- Personnel;
  - Organizations: Units and Nodes;
  - Resources: Holdings,
  - Material,
  - Infrastructure,
  - Information, and
  - Fuel;
- Facilities;
- Capabilities;
- Geospatial Information: Location, Geographic Feature, Area of Interest and Control Feature;

- Actions;

- Context;

- Planning;

- Tasking (Orders);

- Reports: Warnings and Alerts, Suspicious Activity, Status, and Position.

It is up to the community (maritime/harbour security) to determine the domain covered by the COP, and individual decision makers to determine which elements are needed in their decision making process. The community needs to develop the COP for Maritime/Harbour Security.

Each of the information types has a data structure; relationships to other information elements; business rules related to the aggregation and marshalling of the data; and other rules related to information protection and release-ability. This information that underpins the communities understanding of its mandates, roles and responsibilities relating interoperability maritime and harbour security; its ability to assess capability; its ability to identify gaps and areas that need strengthening; and its ability to identify areas that enhance capability.

Activities: The following activities need to be completed as part of this task:

1. Prepare a work plan and schedule for this task.

2. Conduct a government and industry survey to identify published requirements for the SA/DA domain and/or domain models for the EM, PS and/or C4I.

3. Make recommendations on the applicability of information gathered during Item 2, as it pertains to EM and SA;

4. Prepare a high level concept of operations for the application and deployment of the SA/DA domain model:

   a. A description of information is needed by decision makers in the SA/DA domain;

   b. A description of how issues of information sensitivity (privacy, confidentiality and classification) will be addressed in the domain model; and

   c. A description of how issues of information protection and release-ability will be addressed in the domain model.

5. Conduct a workshop on the findings of items 1-4 to ratify observations and recommendations from the survey. The workshop will also be used to gather community requirements.

6. Develop a concept of operational and conceptual architecture for development a federated/virtualized Maritime/Harbour COP/SA;

7. Develop a information domain model in UML for a federated Maritime/Harbour SA;

8. Develop a roadmap of activities for the completion (if needed), adoption and deployment of the domain model.

9. Conduct a workshop on Domain Model and road map recommendations.

10. Prepare and final report describing the work product from the study; provide strategic advice on the development and deployment of SA/DA capability; and provides a recommended Road Map of activities and initiatives to address the gap or gaps identified in the Study.

11. Prepare Monthly Progress/Status Reports summarizing financial and work plan status.

12. Prepare and delivery presentations on findings and progress to stakeholders.

Deliverables: The following deliverables would be provided as part of this study:

1. Project Work plan;

2. Survey observations and recommendations report;

3. Work Shop 1 materials.

4. Work Shop 1 Report;

5. Work Shop 2 materials.

6. Work Shop 2 Report;

7. Domain Model Concept of Operations;

8. Maritime/Harbour SA Domain Model in UML;

9. Presentations;

10. Final Report; and

11. Progress Reports.

Qualifications: The resource qualifications for this activity include:

1. Knowledge of the EMSIF;

2. Knowledge of and Experience with TOGAF, DODAF and UPDM;

3. Experience developing Domain Models for SA and related operational domains;

4. Experience developing SA/DA domain and/or data models;

5. Experience developing system architectures for interagency operations.

6. Detailed understanding SA for multiagency environments.

7. Significant experience / expertise developing interoperability strategies and standards for multi-agency operations.

8. Significant experience / expertise Consultation, Command and Control System Interoperability.

9. Significant experience / expertise developing recommendations for government agencies in the area of interoperability and system interoperability.

10. Expertise in the development, deployment and application of C4I capability.

11. Knowledge of the evolving open standards in area of emergency management System Interoperability.

12. A Bachelor's degree, as a minimum, in Science, Engineering, or a related discipline from a Canadian University or equivalent from a foreign institution, as determined by the Canadian Centre for International Credentials.

13. Experience / expertise developing and presenting recommendations in the areas of operational, information and system interoperability.

Estimate:

The resource estimate for this activity is 6-9 Person-months.

Resources: 1 Sr. Information Architect

T&L budget of approximately $10-15K.

4.1.3   Performance Measures and Metrics

The performance metrics effort conducted during the preparation for the Harbour Siren exercise is primarily based on qualitative measures. These measures should be transformed into quantitative measures that bridge between a Maritime/Harbour Security Business architecture and the Public Safety Canada (PS) Interoperability Continuum. This effort will provide the community with:

- The ability to objectively measure progress in their ability to interoperate; and

- For individual agencies to perform self assessments on their capacity to interoperate with the community.

Activities: The following activities need to be completed as part of this task:

1. Prepare a work plan and schedule for this task.

2. Conduct a government and industry survey to identify published requirements for the SA/DA domain and/or domain models for the EM, PS and/or C4I.

3. Make recommendations on the applicability of information gathered during Item 2, as it pertains to EM and PS SA;

4. Prepare a high level concept of operations for the application and deployment of the SA/DA domain model:

   d. A description of information is needed by decision makers in the SA/DA domain;

   e. A description of how issues of information sensitivity (privacy, confidentiality and classification) will be addressed in the domain model; and

   f. A description of how issues of information protection and release-ability will be addressed in the domain model.

5. Conduct a workshop on the findings of items 1-4 to ratify observations and recommendations from the survey. The workshop will also be used to gather community requirements.

6. Develop a concept of operational and conceptual architecture for development a federated/virtualized Maritime/Harbour COP/SA;

7. Develop a information domain model in UML for a federated Maritime/Harbour SA;

8. Develop a roadmap of activities for the completion (if needed), adoption and deployment of the domain model.

9. Conduct a workshop on Domain Model and road map recommendations.

10. Prepare and final report describing the work product from the study; provide strategic advice on the development and deployment of SA/DA capability; and provides a recommended Road Map of activities and initiatives to address the gap or gaps identified in the Study.

11. Prepare Monthly Progress/Status Reports summarizing financial and work plan status.

12. Prepare and delivery presentations on findings and progress to stakeholders.

Deliverables: The following deliverables would be provided as part of this study:

1. Project Work plan;

2. Survey observations and recommendations report;

3. Work Shop 1 materials;

4. Work Shop 1 Report;

5. Work Shop 2 materials;

6. Work Shop 2 Report;

7. Domain Model Concept of Operations;

8. Maritime/Harbour SA Domain Model in UML;

9. Presentations;

10. Final Report; and

11. Progress Reports.

Qualifications: The resource qualifications for this activity include:

1. Knowledge of the EMSIF

2. Knowledge of the PS Interoperability Continuum

3. Experience developing performance measures and metrics for operational environment

4. Knowledge of architecture frameworks and the application of metrics to those frameworks

5. Experience developing architectures for interagency operations.

6. Detailed understanding interoperability for multiagency environments.

7. Experience / expertise Consultation, Command and Control System Interoperability.

8. Significant experience / expertise developing recommendations for government agencies in the area of interoperability and system interoperability.

9. Expertise in the development, deployment and application of C4I capability.

10. Knowledge of the evolving open standards in area of emergency management System Interoperability.

11. A Bachelor's degree, as a minimum, in Science, Engineering, or a related discipline from a Canadian University or equivalent from a foreign institution, as determined by the Canadian Centre for International Credentials.

12. Experience / expertise developing and presenting recommendations in the areas of operational, information and system interoperability.

Estimate:

The resource estimate for this activity is 6 Person-months.

Resources: 1 Sr. Analyst

T&L budget of approximately $10-15K.

4.1.4 Target Business Architecture

The Maritime/Harbour Security community is a diverse set of agencies operating at the three levels of governments. It also has a need to align effort with organizations from the private sector. Over the years, each of these organizations and agencies has developed their own systems for addressing their individual mandates and operational objectives. The growing requirement to interoperate with other agencies, in response to new public safety threats is straining the capacity of many agencies.

The community needs to develop a shared blueprint for how these diverse systems (human, mechanical, electronic, etc.) will interoperate in the near, mid and far term. For this the community is seeking the development of computationally and platform independent business model describing the interoperation of agencies in the process, information and systems domain. These blueprints will build on the core process and organizational models developed during the planning phases of Harbour Siren Exercise.

The objectives for the development of the development of the Target Business architecture include:

- Describing the Baseline Business Architecture (current state) in terms of DODAF Views and Viewpoints;

- Developing a Target Business Architecture (DODAF Views), describing the product and/or service strategy, and the organizational, functional, process, information, and geographic aspects of the business environment, based on the business principles, business goals, and strategic drivers

- Analyzing the gaps between the Baseline and Target Business Architectures

- Selecting and developing the relevant architecture views, viewpoints and products that will enable the architect to demonstrate how the stakeholder needs are addressed in the architecture

Activities: The following activities need to be completed as part of this task:

1. Prepare a work plan and schedule for this task.

2. Identify the views and viewpoints needed to describe the business architecture (use EMSIF guidance for this activity).

3. Develop the views and viewpoints for the current (as-is) architecture at the community level (or black box agencies), aligning:

   a. HS Models;

   b. Agency context models (interfaces with other agencies);

   c. Other required information and views;

4. Identify information gaps in the description of the current architecture;

5. Describe the high level concept of operation for the elements of the business architecture;

6. Conduct a workshop (1) to ratify the current architecture.

7. Update current architecture to reflect stakeholder comments.

8. Gather requirements for the target architecture from technical authority identified stakeholders;

9. Develop target business architecture for harbour security;

10. Conduct a workshop (2) to ratify the target architecture.

11. Update target architecture to reflect stakeholder comments.

12. Identify gaps between the current and target architecture.

13. Develop a roadmap of activities for the completion (if needed), adoption and deployment of the target business architecture.

14. Prepare a final report describing the target business architecture, gaps and roadmap elements.

15. Prepare Monthly Progress/Status Reports summarizing financial and work plan status.

16. Prepare and delivery presentations on findings and progress to stakeholders.

Deliverables: The following deliverables would be provided as part of this study:

1. Project Work plan;

2. Survey observations and recommendations report;

3. Work Shop 1 materials.

4. Work Shop 1 Conclusion Report;

5. Work Shop 2 materials.

6. Work Shop 2 Conclusion Report;

7. Domain Model Concept of Operations;

8. Maritime/Harbour SA Domain Model;

9. Final Report; and

10. Progress Reports.

Qualifications: The resource qualifications for this activity include:

1. Knowledge of the EMSIF;

2. Knowledge of and Experience with TOGAF, DODAF and UPDM;

3. Experience developing Domain Models for SA and related operational domains;

4. Experience developing SA/DA domain and/or data models;

5. Experience developing system architectures for interagency operations.

6. Detailed understanding SA for multiagency environments.

7. Significant experience / expertise developing interoperability strategies and standards for multi-agency operations.

8. Significant experience / expertise Consultation, Command and Control System Interoperability.

9. Significant experience / expertise developing recommendations for government agencies in the area of interoperability and system interoperability.

10. Expertise in the development, deployment and application of C4I capability.

11. Knowledge of the evolving open standards in area of emergency management System Interoperability.

12. A Bachelor's degree, as a minimum, in Science, Engineering, or a related discipline from a Canadian University or equivalent from a foreign institution, as determined by the Canadian Centre for International Credentials.

13. Experience / expertise developing and presenting recommendations in the areas of operational, information and system interoperability.

Estimate:

The resource estimate for this activity is 6-9 Person-months.

Resources: 0.5 Analyst, 1 Architect

T&L budget of approximately $10-15K.

4.2   Domain Models

Many information domains identified for the Maritime/Harbour Security Common Operating Picture (COP) are intended to provide a summary of information areas:

- **Emergency Management**: providing a high level overview of information requirements for inter-agency emergency planning, response and recovery in a maritime environment;

- **Public Safety**: providing a high level overview of information requirements for inter-agency public safety planning, response and recover in a maritime environment;

- **Public Security (/Intel)**: providing a high level overview of information requirements for inter-agency public security planning, response and recovery in a maritime environment;

- **Collaboration and Planning**: underpinning the development of planning and collaboration tools that enable multi-agency Maritime/Harbour Security operations.

- **Incident Management**: underpinning the development incident management tools to enable multi-agency Maritime/Harbour Security operations.

- **Resource Management**: underpinning the development resource management that enable multi-agency Maritime/Harbour Security operations.

- **Information Security and Privacy**: underpinning the development of information sharing/release-ability and protection services needed for the community to certify, accredit and operate the information services needed by the community.

- **Security/Privacy Policy Management**: underpinning the development of the security and privacy services that enable multi-agency Maritime/Harbour Security operations.

- **Cyber & Communications SA**: underpinning the development of cyber and communications management services needed by the community to configure, operate and safe-guard core capability.

- **Decision Support**: underpinning the development of support services and aids for EM and PS decision makers.

- **Critical Information Protection**: underpinning the development of services that inform EM and PS decision makers and responders to threats, risks and safe-guards to Critical infrastructure and the potential impact on the incident or event – feeds SA capability.

There are a number of overlaps within and between these information domains. The community needs to iteratively develop how domains are addressed by information systems. The community should seek to develop overlapping domain models in these topic areas that focus of the needs of the Maritime/Harbour Security decision makers). Their task descriptions for each of these efforts would be similar to Section 4.1.2, with durations of between 3-6 months.

Each of these information domains has their own decision support/aid requirements that require common definitions of core elements to be interoperable amongst agencies. Operation centre responding to emergency, crisis and major events are required to address each of these domains and more. Few have common of standard definitions that are specified during development or

acquisition. Many members of the Maritime/Harbour Security community lack the resources or expertise to define these domains on their own. A community effort would be a useful assist.

Interoperability across the full spectrum of Maritime/Harbour Security operations is complex. Breaking down the complexity one piece at a time and aligning the pieces will assist the community in achieving its desire to interoperate more effectively. This report is focussing on only two elements: 1) what is situational awareness (SA) and 2) what information does the community need to rapidly (from the onset of an incident) share the information needed to develop and sustain the COP/SA.

A "**domain model**" is a conceptual model of a domain (field of knowledge, real or imagined world, operation or system). It describes the various entities involved in the domain of interest in terms of definitions, attributes, rules, relationships and facts that characterize them. "Conceptual" infers that the model represents 'concepts' (entities) and relationships between them. A conceptual model is explicitly chosen to be independent of implementation details, such as concurrency or data storage. The aim of conceptual model is to express the meaning of terms and concepts used by domain experts to discuss the problem, and to find the correct relationships between different concepts. The conceptual model is used to clarify the meaning of sometimes ambiguous terms, and ensure that problems with different interpretations of the terms and concepts cannot occur; the differing interpretations of key terms (e.g., situational awareness) cause the software and interoperability challenges to fail. Once the domain concepts have been modelled, the community has a stable basis for subsequent developments in that domain (e.g., CAP-CP, NIEM and EDXL information exchange desired by PS).

An important benefit of a domain model is that it describes and constrains the scope of the various capability developments. The domain model can be effectively used to verify and validate the understanding of the problem domain among various stakeholders of the project group. It is especially helpful as a communication tool and a focusing point between technical and business teams. The domain model should serve as a unified, definitive source of reference when ambiguities arise in the analysis of problems or later during the implementation of reusable components, a repository of the shared knowledge for teaching and communications, and a specification to the implementer of reusable components. A model of a domain should include information on at least three aspects of a problem domain: concepts to enable the specification of systems in the domain; plans describing how to map specifications into code; and rationales for the specification concepts, their relations, and their relation to the implementation plans.

At present, much of the effort (and resources) being expended in the development of capability for the EM and PS communities lacks the unifying elements of a domain model. The result of these efforts has been the development of systems, applications and services that deliver partial capability that fails to align with of other systems, applications and services in the environment.

Developing a single unified domain model for all of the EM and PS domains would be a significant challenge. It is recommended that several smaller efforts be initiated to demonstrate the benefit of domain models to a capability development portfolio. Because these domains overlap, some care should be taken to assure that core concepts are provided a single definition.

4.2.1 Information Sharing / Exchange / Protection / Release-ability Domain Model

At the heart of the interoperability capability is the ability to aggregate and share information in a secure and trusted manner. This ability is predicated on an ability to translate mandates, policy, MOUs and SLAs into a set of rules that are enforceable by the IM systems, applications and services deployed to support EM capabilities such as situational awareness, collaborative planning and decision support.

The information sharing, protection and release-ability services are information services in their own right – which capture, collate and execute business rules that govern IM elements of EM operations. These rules constitute an information domain comprising:

1. Information semantics;

2. Aggregation, Marshalling and Storage;

3. Publication and subscription participants;

4. Communities of Interest;

5. Quality of Service Characteristics;

6. Threats, Risks and Safeguards;

7. Guards;

8. Filters;

One of the challenges in the delivery of interoperable IM capabilities (systems, applications and services) is that there isn't a community-agreed structure for this critical information; making the development of design tools and capability is extremely difficult. In addition, these tools and capabilities are typically proprietary and rarely portable across domains.

DRDC is seeking to develop Information sharing/exchange/protection/release-ability Domain Model for the EM community; one that will support the development of portable interoperability solutions.

Activities: The following activities need to be completed as part of this task:

1. Prepare a work plan and schedule for this task.

2. Conduct a government and industry survey to identify published Information sharing/exchange/protection/release-ability policies and requirements as they pertain to the EM and PS domains; in particular the sharing and release of sensitive information (private, confidential and classified) in a multi-agency environment (multiple levels of government and the private sector).

3. Develop recommendations for the information elements gathered in Item 2 and their applicability to the EM and PS community.

4. Prepare a high level concept of operations for the application and deployment of the Information sharing/exchange/protection/release-ability Domain Model.

5. Conduct a workshop on the finds of items 1-4 to ratify observations and recommendations. The workshop will also be used to gather community requirements.

6. Develop a concept of operational and conceptual architecture for development a Information sharing/exchange/protection/release-ability Domain Model;

7. Develop the Information sharing/exchange/protection/release-ability Domain Model;

8. Develop a roadmap of activities for the completion (if needed), adoption and deployment of the domain model.

9. Conduct a workshop to present and ratify the domain model; and describe possible roadmap elements.

10. Prepare and final report describing the work product from the study; provide strategic advice on the development and deployment information sharing Capability; and provides a recommended Road Map of activities and initiatives to address the gap or gaps identified in the Study.

11. Prepare Monthly Progress/Status Reports summarizing financial and work plan status.

12. Prepare and delivery presentations on findings and progress to stakeholders.

Deliverables: The following deliverables would be provided as part of this study:

1. Project Work plan;

2. Survey observations and recommendations report;

3. Work Shop 1 materials.

4. Work Shop 1 Report;

5. Work Shop 2 materials.

6. Work Shop 2 Report;

7. Domain Model Concept of Operations;

8. Information sharing/exchange/protection/release-ability Domain Model;

9. Final Report; and

10. Progress Reports.

Qualifications: The resource qualifications for this activity:

1. Knowledge of the EMSIF;

2. Knowledge of and Experience with TOGAF, DODAF and UPDM;

3. Experience developing Domain Models for SA and related operational domains;

4. Experience developing requirements for environments that capture, process, store and use sensitive (policy protected) information;

5. Experience developing Domain Models;

6. Experience developing rules based systems for EMSI;

7. Experience developing system architectures for interagency operations.

8. Detailed understanding SA for multiagency environments.

9. Significant experience / expertise developing interoperability strategies and standards for multi-agency operations.

10. Significant experience / expertise Consultation, Command and Control System Interoperability.

11. Significant experience / expertise developing recommendations for government agencies in the area of interoperability and system interoperability.

12. Expertise in the development, deployment and application of C4I capability.

13. Experience developing community level domain models.

14. Knowledge of the evolving open standards in area of emergency management System Interoperability.

15. A Bachelor's degree, as a minimum, in Science, Engineering, or a related discipline from a Canadian University or equivalent from a foreign institution, as determined by the Canadian Centre for International Credentials.

16. Experience / expertise developing and presenting recommendations in the areas of operational, information and system interoperability.

Estimate:

The resource estimate for this activity is 6 Person-months.

Resource: 1 Sr. Information Analyst/Architect

T&L budget of approximately $10-15K.

4.3 High Risk Interoperability Services

There are several areas in the interoperability domain that many communities are identifying as too difficult to address. Many are heading down technology paths that lead to dead-ends and the development of shelfware (systems and applications that fail to deliver operational capability and are shelved by users). Several key gaps in current capabilities (standards and technologies) are hindering the development of the flexible and adaptive systems needed to support the communication, information sharing, situational awareness and collaboration. Those services often identified as capability shortfalls include:

- Adaptive communication services:
    - Communications (i.e., radios)
    - Networks
    - Information Exchange and middleware:
        - Dynamic Communities of Interest
        - Data Aggregation Services
        - Tagging and labelling standards
        - Tag and label Processing/enforcement Services
        - Information Protection Policy Enforcement (Privacy) Services
    - Information Security Policy Development/Enforcement;
- Community Semantic for information exchange / Messaging (CAP, NIEM, EDXL, Other)
- Information Domain Virtualization
- Interagency interoperability Testing
- Web based Training and Exercises

Although not a complete list of gaps, delivering standards and technologies in these areas would dramatically improve the community's capacity to develop and deploy system interoperability and the SA desired by Harbour Siren participants.

There are numerous standards and technology efforts in the areas of adaptive communications (e.g., Software Based Radio [SBR]) and networks (e.g., intelligent agents and programmable routers). It is that next layer in the technology stack that needs community attention. From this study it is recommended that the community begin to experiment, demonstrate and test strategies to develop and deploy adaptive data services – targeting COP/SA.

4.3.1 Adaptive Information Exchange Prototype

For the last decade or more, Maritime/Harbour Security stakeholders (decision makers) have been seeking access to quality information in order to make better decisions during planning, response and response operations. Traditional information systems are proving too rigid and brittle to interoperate with the expanding information domain of security operations. The idea of providing the right information to the right person at the right time is as pertinent and elusive today as it was more than a decade ago. The appeal for quality information was expressed by the Harbour Siren participants in terms of a need for better situational awareness during the course of the exercise.

The international community now identifies "Quality Information" as having the following characteristics:

- **Accurate**: semantics to accurately convey the perceived situation.

- **Relevant**: information tailored to specific requirements of the mission, role, task or situation at hand.

- **Timely**: information flow required to support key processes, including decision making.

- **Usable**: information presented in a common, easily understood format.

- **Complete**: information that provides all necessary (or available) information needed to make decisions.

- **Brief**: information tailored to the level-of-detail required to make decisions and reduces data overload.

- **Trustworthy**: information quality and content can be trusted by stakeholders, decision makers and users.

- **Secure/protected**: Information is protected from inadvertent or Malicious Release or use.

The maritime/harbour security community needs the capacity to explore these concepts as a prelude to the adoption of the Public Safety's initiatives to adopt and deploy standards based information sharing services based on:

- Common Alerting Protocol (CAP) Canadian Profile;

- National Information Exchange Model; and

- Emergency Data Exchange Language.

Using Open Standards, and where available open-source software applications, develop a prototype for a dynamically adaptable information sharing service that demonstrates the following characteristics:

- Selective sharing of Information between participants based in architectural patterns exchange patterns integrated into the Harbour Siren Models.

- Selective activation, de-activation and modification (new information elements and new participants) Communities of Interest during the execution of a scenario.

- Aggregation of data to architecture defined sharing patterns;

- Information Protection Policy Enforcement (Privacy) Services.

- Information sensitivity Tag and label Processing/enforcement during aggregations.

- Messaging multiple community semantics (CAP, NIEM, EDXL, Other).

- Alignment with a community common operating picture and SA capability.

- Flexibility and agility during the design, development and operation of the services.

- Opportunity for the integrated service specifications to become open-standards.

The demonstrations of the service should use the Harbour Siren MSEL and Process model as the basis for (digital) information sharing amongst the participants in a Maritime/Harbour Security

Activities: The following activities need to be completed as part of this task:

1. Prepare a work plan and schedule for this task.

2. Prepare a white paper on how the service characteristics will be addressed.

3. Conduct a short government and industry survey to identify open technologies and standards to be used for the prototype.

4. Prepare a platform Independent model for the prototype.

5. Prepare a high level concept of operations for the application and deployment of the Information sharing/exchange/protection/release-ability Domain Model.

6. Conduct a workshop on the finds of items 1, 2 & 3 to ratify observations and recommendations from the survey.

7. Develop a concept of operational and conceptual architecture for development of an Information sharing/exchange/protection/release-ability Domain Model;

8. Prepare and final report describing the work product from Tasks 1 to 4; provides strategic advice on the development and deployment EMSI Capability; and provides a recommended Road Map of activities and initiatives to address the gap or gaps identified in the Study.

9. Prepare Monthly Progress/Status Reports summarizing financial and work plan status.

10. Prepare and delivery presentations on findings and progress to stakeholders.

Deliverables: The following deliverables would be provided as part of this study:

1. Project Work plan;

2. Survey observations and recommendations report;

3. Work Shop 1 materials.

4. Work Shop 1 Conclusion Report;

5. Domain Model Concept of Operations;

6. Information sharing/exchange/protection/release-ability Domain Model in UML;

7. Final Report; and

8. Progress Reports.

Qualifications: The resource qualifications for this activity:

1. Detailed Knowledge of the development of COP and SA capabilities;

2. Knowledge of Information Assurance and Privacy other issues affecting COP and SA

3. Knowledge of international and national efforts to develop and deliver COP and SA in multi-agency and/or coalition environment.

4. Knowledge of the EMSIF;

5. Knowledge of and Experience with TOGAF, DODAF and UPDM;

6. Experience developing Domain Models for SA and related operational domains;

7. Experience developing Domain Models;

8. Experience developing rules based systems for EMSI;

9. Experience developing system architectures for interagency operations.

10. Detailed understanding SA for multiagency environments.

11. Significant experience / expertise developing interoperability strategies and standards for multi-agency operations.

12. Significant experience / expertise Consultation, Command and Control System Interoperability.

13. Significant experience / expertise developing recommendations for government agencies in the area of interoperability and system interoperability.

14. Expertise in the development, deployment and application of C4I capability.

15. Knowledge of the evolving open standards in area of emergency management System Interoperability.

16. A Bachelor's degree, as a minimum, in Science, Engineering, or a related discipline from a Canadian University or equivalent from a foreign institution, as determined by the Canadian Centre for International Credentials.

17. Experience / expertise developing and presenting recommendations in the areas of operational, information and system interoperability.

Estimate:

The resource estimate for this activity is 6-9 Person-months.

Resources: Information Analyst, Architect, programmer analyst and programmer

T&L budget of approximately $10-15K.

4.4   Open Standards Development

Many of the definitional efforts described in this roadmap have the potential to help a broad community on the international stage. The requirements for maritime emergency, crisis and major event planning, response and recovery, form an information system perspective, are quite similar. There is growing interest in the development of open, international standards in these areas. OMG, OASIS, NIEM and others already have on-going efforts in this area and would welcome greater participation and community direction.

From proposal to acceptance the standardization takes between 18 and 30 months provided there standards body members interested in contributing to the development of the standards. The efforts follow the following steps:

- Task Force Agreement to process

- RFP Preparations

- RFP Approval and Release

- Letter of interest from contributors

- Initial submissions

- Revised submissions (and amalgamations of individual submissions)

- Final Submissions

- Preliminary adoption

- Broad community review and finalization

- Adoption

Each group varies slightly but follows similar practices.

The community should fund participation in the appropriate standard bodies to ensure the maritime/harbour security requirements are accounted for in the evolving standards. This could be addressed by funding the participation of trusted consultants for the individual meetings. Short term contracts comprising:

- Short review of community priorities;

- Meeting attendance (including Travel and Living);

- Summary report and presentation on findings

Estimate:

The resource estimate for this activity is 7 - 10 days per meeting.

Resources: Sr. Analyst or Sr. Architect

T&L budget of approximately $3-5K.

5   Conclusion

The analysis provided recommendations related to: 1) the EMSI Capability Portfolio, focusing on the development/deployment voice and data interoperability capability; and 2) on Exercise Process Improvement, focusing on improving exercise planning, executions and assessment. The recommendations build on the Harbour Siren observations and provide strategies for the community to develop greater capability, flexibility, agility and adaptability in their ability to interoperate. Key areas include: A) shared community vision for voice and data communication; B) shared community understanding of requirements resulting from this shared vision; C) provision of shared situational/domain awareness; and D) enhancement of interagency collaboration.

Near-term roadmap activities were proposed in the areas of business architecture, domain models, high-risk interoperability services and open standards development. Many of these recommendations are aimed at the R&D community, in support of the Emergency Management community. The recommendations should be useful to DRDC Centre for Security Science to develop and prioritize research projects in these areas.

DRDC Atlantic CR 2010-179

References

[1] Defence Research and Development Canada, "Preliminary Report on Metrics Development for Inter-Agency Maritime Emergency Response Operations: Harbour Siren 2009", DRDC Atlantic CR 2009-262, July 2010

[2] Defence Research and Development Canada, " Inter-Agency Harbour Security Model Update: Harbour Siren 2009", DRDC Atlantic CR 2009-263, July 2010

[3] Defence Research and Development Canada, "Harbour Safety and Security Process Mapping: IMSWG", DRDC Atlantic CR 2010-196, May 2011

[4] Defence Research and Development Canada, "Improving Marine Safety and Security: Lessons from Harbour Siren", DRDC Atlantic CR 2010-180, May 2011

[5] Defence Research and Development Canada, "Harbour Siren: Technical Recommendations Report", DRDC Atlantic CR 2010-179, May 2011

[6] Public Safety Canada, "Who's on First? Table Top (TTX) After Action Report", December 10, 2008

[7] Public Safety Canada, "Exercise Harbour Siren: After Action Report (AAR), March, 2010-06-03

[8] Public Safety Canada, "Harbour Siren Exercise: Evaluators Guide", October 2009

[9] Public Safety Canada, "Harbour Siren Exercise: Exercise Design Team Guide", October 2009

[10] Public Safety Canada, "Harbour Siren Exercise: Player Handbook", September 2009

[11] Public Safety Canada, "Harbour Siren Exercise: Major Scenario Event List (MSEL)", September 2009

This page intentionally left blank.

Annex A Harbour Siren 09 Observations

Ref.	Identifier	Observation	Impact / Note
1	**Identification of Interoperability Objectives and Targets**	The MSEL, metrics and the process model seem to be focusing on communication interoperability and elements of processes. The after action assessments seem to focus on information interoperability and situational awareness. These elements are not mutually exclusive, but the misalignment makes it difficult to identify specific issues or gaps. Discussion during the March 9th Workshop often referred to a lack domain/situational awareness during the exercise. However, there was not much consistency in the participants description of what was missing or their specific criteria for this assessment. It is quite a challenge to objectively identify GAPS in capability without a general (preferably shared) understanding of what SA/DA means to the community and the individual agencies. It was clear that expectations were not met; it is less clear what these expectations were before, during and after the exercise.	Evaluating everything "interoperability" on a single pass would be extremely difficult and costly to achieve given the number of agencies involved. Interoperability represents the ability of systems, services organizations or people to provide data, information, personnel, materiel, and services to and/or accept the same to enable them to cooperate effectively to meet mission or operational objective. Interoperability can take the forms of: • **Communications interoperability** refers to the ability of emergency responders to share information via voice and data signals on demand, in real time, when needed, and as authorized, or when communications systems are interoperable; e.g., police and fire-fighters responding to a routine incident can talk to each other to coordinate efforts. Communications interoperability also makes it possible for emergency response agencies responding to catastrophic accidents or disasters to work effectively together. Finally, it allows emergency response personnel to maximize resources in planning for major predictable events such as the 2010 Olympics, G8 Summit, or for disaster relief and recovery efforts. • **Network interoperability** refers to the seamless (direct) interconnection of distinct networks so that information and data can circulate efficiently in response to operational needs and service requirements. • **Information interoperability** refers to the ability of two or more computer systems/applications (e.g., situational awareness, collaborative planning and decision support) (/applications) to exchange and process information in a consistent and predictable manner. • **Process interoperability** refers to the ability of two or more agencies can interact without changing internal processes to accommodate inter-agency-operational requirements. • Other areas of where the term interoperability applies: equipment, fuel, etc …
2	**Measurable Objectives**	The reviewed documentation does not clearly identify targets for specific capabilities and abilities to interoperate; The measures should	The conversations during the HS Workshop clearly identified the need for continual (evolutionary) capability improvement program across a

Ref.	Identifier	Observation	Impact / Note
		derive from documented requirements: 1. Legislated Mandates; 2. Policy; 3. SOPs/service level agreements (SLAs); and 4. Stakeholder/user defined needs. Performance measures and metrics also need to be tied to known (agreed) targets, which observed capability can be compared to identify GAPS. It is these observed gaps that EMSI portfolios and/or capability roadmaps are scoped and prioritized for the near, mid and far terms activities. The HS metrics should have been aligned to agreed targets.	number of EMI capability domains. Stakeholder/user and derived requirements need to be aligned with near, mid and far term targets. The community needs common vision (objective) and transition plan for the evolution harbour security interoperability. The technology breakout session identified the need for solid business practices, processes and procedures in advance of technology deployment. Technology needs to meet community/agency objectives; or it can easily be shelved at large $$$ cost to the community. Failed deployments of technology often sour stakeholders desire to collaborate on subsequent efforts. **Notes**: 1. Targets of assessment should be developed at the community level vs. targeting individual agencies. And should have a measurable (PMS) component. 2. Measurements should be aligned with the PSC continuum. This would provide a common presentation and dashboard. 3. Metrics that are potentially traceable to individual agencies and or groups of agencies should be assessed in relation to their mandates, policies and priorities.
3	**MSEL vs. Process Model**	There seems to be differences between the communication flows depicted in the process model and those identified in the Master Sequential Event List (MSEL). The model illustrates parallel data events occurring – and independent action – not depicted in the MSEL. The MSELs focus on Voice (radio/phone) and Fax is not clearly articulated in the Process Model and the process model seems to imply more data exchange.	The difference in the process models and the MSEL seems to illustrate differences in interpretation or expectations. These differences in interpretations or expectations should be address in the exercise models.
4	**Information Architecture**	The reviewed documentation did not capture the information requirements of expectations of the participating agencies. The exercise models should depict: • The content and structure of the information exchanged during the exercise. • The capture, digitization, storage, … of event information … • Any legal impediments to the capture, aggregation or dissemination of information. • What information is available in the environment, who has it, who one can get it, … • The information needs of each of the participating agencies. • What is included in the information set (domain model) for situational (/domain) awareness, what resides where, who needs	There was significant discussion of the need for and lack of situational awareness in the after action reports. This was repeated during the discussion groups as the workshop. What was difficult to assess was the expectations of the individuals making these comments. Was it the availability, timeliness or quality of information that was the issue? Information architecture (domain models) is needed to understand the current and target quality of information (Accuracy, Relevance, Timeliness, Usability, Completeness, Brevity, Trustworthiness and Protected) in the maritime and harbour domains. This should be added to the current process views in the current models. Without expectations (service level agreements) on the part of stakeholders – it is hard to identify the specific gaps in operational information (situational awareness).

Ref.	Identifier	Observation	Impact / Note
		it, … • Expectations on a participant's capacity to produce and/or share information underpinning the tactical and operational pictures; the basis of situational (domain) awareness and decision support. This would really assist in the discussions relating perception of poor situational awareness amongst community members.	
5	**Technical Architecture**	The reports provided little insight into the deployed technology for each of the participating agencies or the capacity of the agencies to capture, aggregate, process or share information. This information would provide a baseline for GAP analysis and the development of capability roadmaps. Catalogue of each participant's technical (COMMS, network, platform, middleware, information holdings and applications) infrastructure would be a useful outcome of exercise like HS.	The information comprising a technical architecture is needed to assess the current (AS-IS/start) state of the environment for the development of capability roadmaps.
6	**Business Architecture**	The reviewed document did not provide the SOPs and service level agreements that address the resource needs (e.g., information) of partner agencies. Catalogue of each participant's SOPs and SLAs would be a useful outcome of exercise like HS.	
7	**Resource Needs**	The reviewed documents provide little indication resource (enablers- data, information, personnel, materiel, and services) needs of the participating agencies or how/where these needs are being met.	Important information in the analysis of GAPs and the development of roadmaps. There was an excellent point made during the technical breakout session during the March 9th HS workshop: The challenges to delivering the capacity to interoperate across large cross sections of the community will be developed one issue at a time. The "BIG Bang" for fixing the universe is highly unlikely in this diverse a community. The more individual challenges that are specifically identified – the faster they can be addressed. It is important that issues be documented and added to the various S&T, community and agency roadmaps. Understanding expectations (/needs) is an important step in identifying and prioritizing efforts.
8	**Communities of interest /practice**	The reviewed documents provided did not illustrate information exchange patterns (communities of interest (CoI)/communities of practice (CoP)) for the partners to the exercise.	CoIs/CoPs assist in grouping needs and the development of capability. Priority can also be to larger CoI as solving it needs to address a broader cross section of the community and return more for the invested $$$. In additions these information sharing patterns can be used to establish initial communication configurations at the start of a response. The community would not have to determine the basis patterns from scratch each time. The ability to setup, modify and tear-down communities of interest based on information needs and release-ability restrictions is an important tool for interoperability. Community members need to be

Ref.	Identifier	Observation	Impact / Note
			able to join and withdraw from CoI rapidly in response to changes in operational context, role, ...
9	**High reliance on Voice COMMS**	The MSEL focussed on voice and fax based communications. There seems to be a gap between the community and public safety's (interoperability directorate) desire to move to information centric (CAP, NIEM, EDXL, ...) SA and the communities reliance on voice.	
10	**Expectations / Outcomes**	The reviewed documents provide little guidance on the expected results (response, outcome) of an event and how each event affected each agency. The documents did not identify how, or if, critical information is expected to be communicated between agencies and operational nodes. It was unclear: as to who was responsible for informing each of the agencies or if individual agencies needed to be informed. In addition, operational activities often occur in parallel and chain from one to another in an asynchronous manner. It is difficult to assess from the which agencies were supposed to get resources (e.g., information), who were not, who was responsible for providing the resource, where there alternate sources for the resources, ..., what were stakeholder expectations in these areas?	During the March 9th workshop, several participants identified the high resource cost in maintaining distribution lists within their own organizations, let alone, those for their partners. The development of a strategy, process and technology for managing information distribution would be very useful. The supporting materials for an exercise need to address the information quality (Accuracy, Relevance, Timeliness, Usability, Completeness, Brevity, Trustworthiness and Protected (sensitivity, release-ability, ...)) – this is at the heart of interoperability and the expectations of decision makers. Is there a document containing stakeholder expectations; or a vision statement (s); or a concept of operations; etc ...
11	**Backup Communication Channels**	The reviewed documents do not identify backup or redundant channels for communication between agencies. During the March 9th WS, several participants identified that information was missed or changes to information not effectively reported.	Important capability – as things inevitably go wrong.
12	**Non-repudiation**	The reviewed document made no mention of mechanisms for non-repudiations - to assess whether communications were missed, not receive, not understood, not aligned to receivers capability, sent to the wrong node, ...	This capability identifies when things go wrong.
13	**Common understanding of shared Situational or Domain Awareness**	Both the reviewed documents and conversations at the HS workshop identified challenge developing and maintaining situational awareness.	SAFECOM identifies interoperability as: "Interoperability is the ability of emergency responders to work seamlessly with other systems or products without any special effort. Wireless communications interoperability specifically refers to the ability of emergency response officials to share information via voice and data signals on demand, in real time, when needed, and as authorized" Communication interoperability is insufficient for the SA/DA, which needs an interagency ability to share information that can be received, parsed, aggregated, integrated and processed by information and decision-support systems being sought by stakeholders. For this extended SA/DA capability the community needs a common understanding of the domain and a common vocabulary.

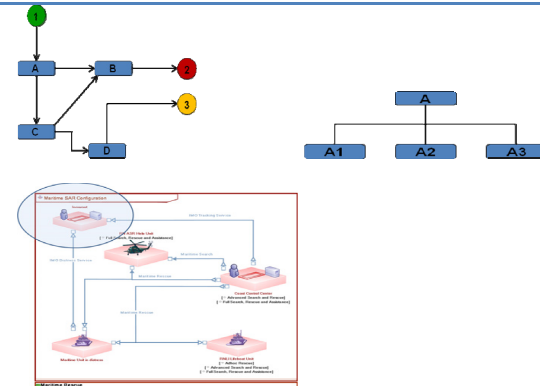| Ref.	Identifier	Observation	Impact / Note
			PSC is seeking to broaden the use of information standards such as the National Information Exchange Model (NIEM) and Common Alerting Protocol (CAP) Canadian Profile to enhance situational and/or domain awareness. This will provide a vocabulary – though it needs to be agreed by the participating agencies. In addition, developing and maintaining SA/DA will require the community to articulate of their meaning of situational or domain awareness, including: 1. The information comprising DA/DA (develop a domain model of primary concepts); 2. The rules governing the capture, use and release of this information; 3. Roles and responsibilities for the collection, aggregation, processing and dissemination of the information; and 4. The services (capabilities) required to capture, store, aggregate, protect (privacy, confidentiality and security) disseminate information. During the technology breakout session of the March 9th HS workshop, participants identified that it is difficult to articulate SA and DA requirements. They needed the opportunity to experiment with various capabilities – and that this **must not be tied** to a single vendor or technology (procurement and maintenance risks would result). Capabilities demanded by the community must be within the development option of all vendors.
14	**Metrics need to be aligned to a harbour security business Architecture**	The metrics (ref. 1) was not tied to business, operational, information, technical and communications architectures elements. Currently they are primarily tied to process elements. Though a good starting point – the metrics need to extended and aligned to measure performance in all elements of interoperability.	Performance measures and metrics should help to seek to isolate GAPs to architectural elements: Processes, Communications, Networks, Middleware, etc. This will help target and prioritize development activities and resource allocations.
15	**Metrics aligned to the Interoperability Continuum**	At the other end of the spectrum, the metrics should align to the PSC interoperability continuum. This would provide a common dashboard through which exercises and stakeholders can express their capability in a consistent manner.	This alignment will guide a performance measurement (PMS) development effort for Emergency Management System Interoperability (EMSI) and Public Safety (or security) system Interoperability (PSSI). The Communication interoperability Continuum addresses: 1. Governance 2. Operating Procedures 3. Data Communications 4. Voice Communications 5. Training and Exercises 6. Usage (of deployed capabilities)

Ref.	Identifier	Observation	Impact / Note
			To support the CAP, NIEM and EDXL initiatives, PSC extended the continuum into the IM domain. These extensions are provided in the Information Interoperability Continuum: 1. Governance 2. Operating Procedures 3. Information Management 4. Information Protection and Security 5. Information Sharing 6. Platform, Infrastructure, Security and Communications 7. Architecture 8. Training and Exercises 9. Usage (of deployed capabilities) Best practices, techniques and tools will be needed to support higher levels of information sharing in a manner that provides the flexibility, agility and sustainability needed by the community – and where capability is developed at levels that enable agencies at varying technology capacities.
16	**Exercise Planning and development Process**	The materials (references) provided for a good starting point for the development of a process for planning, developing, executing and assessing tabletop and operational exercises; build on one to the next.	The goal should be repeatable/managed process for planning, executing and assessing multi-agency interoperability exercises in line with the capability evolutions expresses in the continuum. The process should apply the National Exercise Program guidelines and tools. The process should focus on capturing, documenting and assessing capability at the boundary points of stakeholders – Avoid temptation to look into the black box unless invited in.
17	**Lessons Learned**	As indicated in the Auditor General's report and comments of a large number of community members (publically and privately): "The challenges and lessons learned are not followed up post exercise or operations. And the same challenges reappear time after time."	The experimentation, demonstration and development portfolio must be tied to the to the lessons learned, RISKS and Challenges identified during exercises and operations (See Recommendations: Risk Registry)

Annex B Emergency Mangement and Systems Interoperability Observations

Ref.	Identifier	Observation	Impact / Note
18	**Vision**	The reviewed documents do not present the common or shared vision of interoperability for harbour security to which the stakeholder objectives should be measures. The documents provide a general discussion of interoperability and SA; but no specific requirements for maritime/harbour security. Much of the vocabulary takes and military tone that is not representative of the EM community. The community needs to participate in expressing interoperability needs and vision in their own vocabulary and context.	A shared vision set expectations for the community, observers and evaluators. It will enable the evaluation of capability within the context of the community and the individual partners. If "voice" is all that is required by an agency and its partners and it is available – an inability to receive and process CAP messages is not an indicator of a gap in capability. Context is very important in a assessment of capability.
19	**Common Vocabulary**	Operational use of a common vocabulary for data dissemination was not assessable from the documentation.	The GC has several but no common or shared vocabulary, taxonomy or ontology for Emergency Management, Public Security, or Public Safety. This will be a challenge as the community move the semantic interoperability target of blended CAP, NIEM, EDXL ... environment. Death by acronym – is also a growing challenge as the numbers of agencies expands. With the PSC challenge of semantic interoperability – automated sharing and processing of information –the development of a shared vocabulary is essential.
20	**Core Concepts, Vision and business architecture**	Conversations at the HS workshop indicated that Stakeholders, decision makers, practitioners and users have varying appreciations of the core concepts for harbour security (EMSI), which differs in many ways from operational procedures. There does not appear to be: • A Common level of appreciation of the levels of situational/domain awareness that can be achieved in the maritime/harbour domains • An expression of information needs for various decision points and decision makers during the HS events. Neither what is possibly available – what is needed? • An expression of interoperability requirements for the community collaboration (e.g., joint planning and tasking) during the planning, response and recovery stages of an incident. • An expression of what information is expected to be available at the reporting of an incident, at a hand-over, ...	These data and information views need to be integrated into the architecture models. Architecture based methods for capturing this information need to be demystified for the community and blended into the toolkits of stakeholders. Business analysts from the partnering agencies need to collaborate on the development of these architectural models.
21	**First Principles and Basic**	In a number of areas the community seems to be running ahead with technology development of selections. These efforts are often falling short basic science (systems engineering) discipline that make capability	This has and continues to be a major failing across the Information Management and Information technology domains. The community need to adopt some simplified practices (guidelines, processes and tools) that provide

	Science	project successful. S&T activities have core set of principles need to be completed: Processes that have to be completed before anything else can happen. Engineering provide us many foundational concepts. However, in the area of "interoperability" many of these systematic practices are being ignored, E.g.: • A clear set of requirements from stakeholders. • Clear understanding of the domain: • Seeking to build a complex systems without blueprints; • Make decisions without access to relevant information • Share data without details on how to process, store or safeguard it. • Sharing e information without and defined vocabulary (language or basic concepts); • ... other This typically often results in the development of capability/systems that are costly, unsustainable, useable, unreliable, brittle, ... and Users that turn them off because they are too difficult to use.	stakeholders with the ability to describe and document their interoperability needs and share them with partnering agencies. These practices should permit the analysts, architects and developers augment these descriptive models, and generate the specifications needed for acquisition or development of capability. The EMSIF is beginning to provide guidance in these areas. These efforts should leverage international or open standards to assure that stakeholders have the appropriate tools support.
22	**Sensitive Information**	There is much mythology around the collection, processing, handling and sharing of information. Sharing sensitive information(private, confidential, caveated, classified) is a reality of maritime/harbour security and the processes, constraints, and safeguards needed to protect sensitive information.	Currently a show stopper to interoperability. Policies, Strategies and technologies for the handling and sharing sensitive information during multiagency operations needs to be addressed. In many cases the issues are being addressed until the lawyers get involves (too late) – or being an excuse for not addressing interoperability. In an emergency, information not normally shared is allow to be shared – practices, processes and technologies to enforce these EM and PS regulations in the maritime/harbour domains. Liaison offices work in small operation – but with 50+ agencies involved it is an impractical approach. Policy enforcing technologies (with human in the loop or overrides) are required.
23	**Architecture**	HS process models are a good start to the "as is" architecture for a harbour event. These models need to be augmented with a set of: 1. strategic (capability) views illustrating current capabilities 2. information views depicting the information holding of the agencies in reference to a harbour event, its release to other agencies, the need of other to have that information 3. organization-relationship views depicting the formal and informal relationships (/communications) between the participating agencies 4. Technology views illustrating the technologies deploy by participating agencies that of interoperability options. 5. Standards Views identifying the interoperability standards deployed by participating agencies (e.g., emailing DOCX files versus DOC file may be the difference in being or not being interoperable).	Architecture is the process for developing blueprint capabilities expected by stakeholders. Many development, acquisition and exercises fail to deliver blueprints in an manner that effectively tie key elements together for analysis or assessment. This hampers efforts like HS to enhance community capability. Additional effort is required each time to develop and understanding of what is or supposed to be; costing time and resources. In general, the notion of architecture conjures up visions of teams of 100s of analysts/architects working for years to define this that will never be. Stakeholders are reluctant to adopt architecture techniques because they do not see a real ROI. But then again, stakeholder would never agree to spend $Ms on a building without their experts approving the blueprints; yet $Ms on mission critical information systems that do not follow the same rigor. The result: the stakeholders do not retain the foundational information needed to test, certify and effectively maintain capability. In reality – stakeholders, decision makers and practitioners do architecture stuff all the time (see pictures).

	6. Dictionary View providing and common vocabulary, taxonomy, ontology, ... for maritime/harbour EMSI Exercise like HS also need a blueprint of what stakeholders need – to assess the gaps. Assessment against what is (as-is) identifies things that are mis-aligned or broken. Assessment of target quantifies or qualifies gaps for future capability development.	 The community simply does not capture align and leverage the resulting information. Most of this is done on napkins and white boards, captured in PowerPoint and Visio and lost in the archives.	
24	**Integration vs. Interoperability**	A conversation during the workshop shows a general confusion about the differences between integration and interoperability (the target). The terms are use often used interchangeably (typical for the IT community). This has been caused by decades of the IM community using the terms interchangeably. This is causing a fear that efforts to deliver interoperability will cause significant changes to their internal IT environments. The majority of participants in the workshop identified this as a risk and a detractor to participation.	Basic information is provided in attachment A.
25	**Risks, Challenges and Lessons Learned**	There does not appear to be central registry for cataloguing the Risks, Challenges and Lessons Learned that HS could use. Many of the Risks, Challenges and Lessons Learned are identified repeatedly during operations, exercises, development, testing, … Comment by participants and multiple PSC meetings, including the March 9th HS workshop, identified that this lesson learned are rarely auctioned. Community members also need a place where they can Identify their evolving or deployed solutions to, or risk mitigations strategies for challenges to the development, deployment, operations and maintenance of Communications, interoperability, etc …	HS needs to post its lessons learned and identify the resulting actions. The portal page should be accessible to all HS participants – providing the opportunity to comment.

This page intentionally left blank.

Annex C   Recommendations

C.1   Maritime EMSI Capability Portfolio

Ref.	Title	Description	Comments
1	**EMSI / Interoperability Vision and Business Architecture**	The Maritime/Harbour Security Community requires business architecture to align and manage its EMSI portfolio and coordinate capability development. The business architecture should comprise: 1. Overview and Summary **(Alignment of Current Document)** - **For maritime/harbour security and EMSI** 2. Strategic Capability Transformation (Vision) 3. High Level Operational Concept (including Security / Privacy Concept) 4. Integrated Dictionary **(extension of Current Documentation)** 5. Information Domain Model (Conceptual / Logical)l 6. Operational Resource Flows **(Alignment/Extension of Current Model)** 7. Organizational Relationships **(Alignment/Extension of Current Model)** 8. Operational Activity Decomposition **(Alignment of Current Model)** 9. Operational Rules and performance measures 10. Standards Profile See Attachment be for the alignment of architectural elements.	This recommendation addresses elements of the HS observations: 1, 2, 4-9, 13-15, 18-20, 23 As illustrated, the current documents and models provide much of this information. It is recommended that between exercises the community align and augment this information – to provide an common/shared vision and business architecture for **maritime/harbour security and related EMSI.** TOGAF defines an Architecture Development Methodology (ADM), endorsed by TBS, that is foundational to the EMSIF. TOGAF ADM describes a process for the development of architectures to solve complex business challenges such as maritime/harbour security interoperability. The first steps describe stakeholder vision and business needs as part of a set of architectural views. This can be converted in to a capability development portfolio by aligning this information to a set of capability views: 1. Strategic Capability Transformation (Vision) 2. Capability Dependencies 3. Capability Phasing (Transformation Plan) 4. Capability to Organization Allocation 5. Capability to Activity Mapping The architecture should delineate the boundaries between community and agency responsibilities and controls; reducing friction and overlap – and providing better coordination during expansion or escalation of an incident. In general terms, an architecture describes the entities (objects, etc.) operating in a specific domain (environment) and how they are supposed to interact. Maritime/Harbour Security represents a complex multifaceted environment that necessitates the alignment of government and private sector resources into overlapping communities of interest, capabilities and practices. The alignment of these facets cannot be effectively staged at the onset of an incident; existing knowledge, planning and training must be present. The Maritime/Harbour Security vision and business architecture needs to address the wide range of incidents (or incident types), for multiple ports, and jurisdictions, including: o Vessel fire/explosion alongside; o Vessel fire/explosion in stream or at anchor; o Collision; o Grounding;

|			
			o Oil spill; o Bridge collision; o Vessel adrift; o Bomb threat; o Refinery fire; o HAZMAT spill (other than oil); o Shore-based HPA facility fire/explosion; o Shore-based non-HPA facility fire/explosion; o Grain elevator fire/explosion; o Radioactive material incident; o Nuclear power vessel incident; o Hostage; o Jumper (prior to water entry); o Body in water; and o Search and Rescue (SAR). The architecture needs to illustrate how varying configurations of organizations can align its processes, people, capabilities and resources (including information) to respond to and recover from an incident. The architecture also needs to illustrate options for agencies to align capability while retaining IM/IT investments and Operating procedures. The architecture should provide traceability to stakeholder requirements and lessons learned.
2	**Information Domain Models**	A core element in the architecture is the information domain model for comprise maritime/harbour security situational awareness (MHSSA). This domain model would identify and describe the information elements comprise MHSSA and the relationships between these elements. The MHSSA domain model will align elements of: • Maritime and Harbour Situation/Domain Awareness. • EMSI and PSSI • Collaboration and Planning; • Cyber & Communications Security. • Decision Support; and • Critical Infrastructure Protection.	This recommendation addresses elements of the HS observations: 1, 4, 6, 8, 22 To obtain a community wide view of the situation awareness and coordinate an effective response to incidents, SA information must be shared amongst stakeholders from all sectors. The stakeholders include federal, provincial, and municipal government departments; industry; and in some instances international partners. This in turn means that each of these partners requires a shared understanding of the information environment underpinning situational awareness – What information does each partner need to provide to the community to develop the COP, under what circumstances is this information provided, under what legislation or mandate and how is this information going to be used and safe-guarded. The development of information Interoperability strategies, capabilities, systems and services is predicated on a shared community understanding what information (voice, data) is needed to address decision points in the business or operational processes. The community needs a shared understanding of content, semantics, sensitivity and release-ability for information holdings within and between agencies during various types of incidents. Developing this understanding will also provide a metric for agencies to assess their ability to receive, process and digest this information. Engineering best practices focus on the development of domain models to serve this purpose and form part of the business architecture for the community. These information domains underpin many of the MHSSA capabilities

needed to the planning, response and recovery stages of an event. At present, Public Safety Agencies (world-wide) do developed domain models in these key areas and will be hard pressed to aggregate and process data in a manner that enables decision makers.

As Public Safety Canada integrates other standards like CAP(CP), NIEM, EDXL …, the lack of this foundational work will make it increasingly difficult to align these standards into the information domains of the agencies. These XML schemas do not provide the business rules for aligning the information to the SA/DA, decision support, GIS and other information systems used by the community. These mappings need to be supported by the individual agencies. Having at least one community standards would help many of the agencies involved.

It is recommended that DRDC develop a domain model for Maritime and Harbour security awareness that identifies the information needs of community members; to be shared in order to develop the COP; and develop the decision aids necessary to the identification of, planning for, response to and recovery from an maritime security incident. This model should be aligned with a broader effort by PSC to develop a generalized EMSI SA model. The domain model for SA is sorely needed to facilitate ongoing discussions.

| 3 | New Architecture and Engineering Practices | The development of architecture models (blueprints) is essential to the development of large complex systems (e.g., buildings, ships, information systems, and interagency communications). The community needs to adopt a minimal set of architecture constructs that define a common language for sharing architecture information between partners:

 o Objectives, goals and targets;
 o Information holdings;
 o Sensor data;
 o Resources availability;
 o Resource needs/requirements;
 o Technology and standards;
 o SOPs; and
 o Other.

Architecture based methods for capturing this information need to be demystified for the community and blended into a simple toolkit of stakeholders. Business analysts from the partnering agencies need to collaborate on the development of aligned segment architectural models. | This recommendation addresses elements of the HS observation:1, 2, 4-6, 19-23
By its very nature, delivering interoperability across diverse communities is by its very nature – A COMPLEX SYSTEM comprising:

• Large numbers of mandates, roles and responsibilities;
• Large numbers of distinct operating
• Large number of interface
• Large number of technologies and interfaces
• Multiple operational languages
• Other
The goal of interoperability is to bridge these complexities while maintaining the operating integrity of the individual agencies. For this we need a bridging (shared) language for stakeholders to express their capabilities and needs to its partners. This expression of capabilities and needs must be available during prevention/planning/training to assure that capability is capability is available at the onset of an incident or event. The maritime/harbour security community requires the capacity to express (model) capabilities and needs:
 • Interagency interaction (event-response)
 • Communications
 • Interagency Operating Processes
 • Information exchange:
  o Information Sharing agreements
  o Semantics (data patterns) |

- Information Protection (Privacy, Confidentiality and Security)
- Information Quality
- Resource Exchange
- Service Level Agreements
  - Metrics
  - Traceability
  - Audit-ability
  - Analysis
- Technology and Standards

Great attention needs to be paid to the applicability and usability of the architecture practices and techniques – specifically for a community that is not technically inclined. There is a propensity to over complicate the requirements beyond what in essential.

EMSIF identifies adopts the following principles:

- Architecture Framework comprising TOGAF, DODAF and UPDM
- Develop the minimal set of views needed to
- New practices and techniques should be based on, or translated as open standards. It should have access to multiple sources for:
  - Tools
  - Training
  - Mentoring
  - Other Resources
- Practices should align (following figures) legislation and policy requirements to elements of deployed capabilities; enabling verification and certification (Privacy, C&A and Verification and validation).
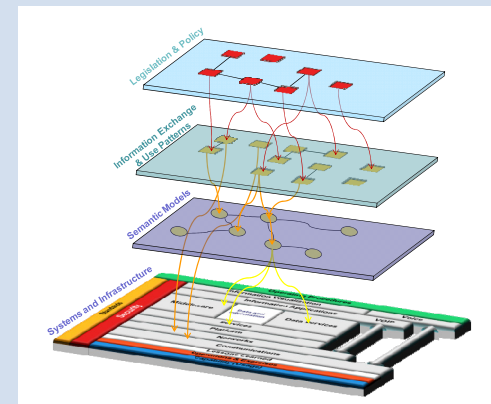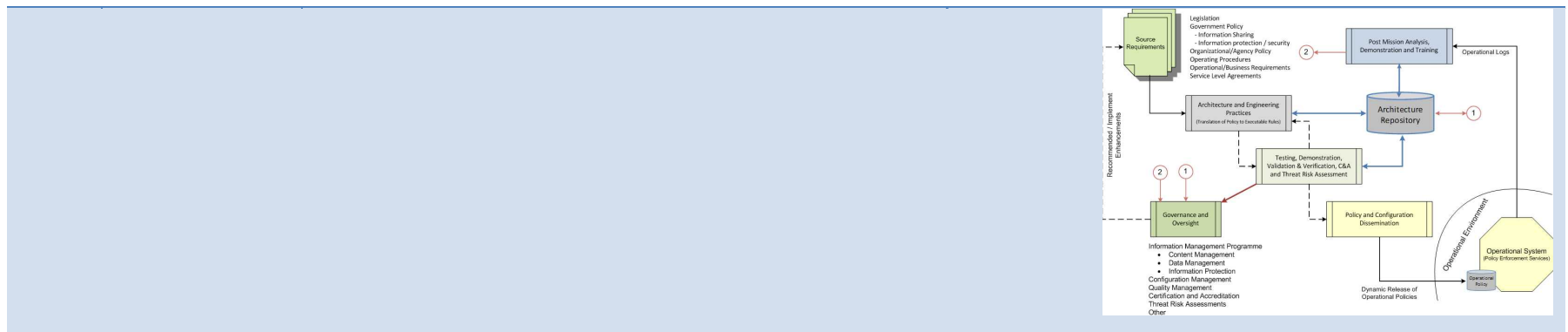
| 4 | **High Risk Interoperability Services** | There are currently major gaps in the knowledge and technology base needed to develop, deploy and sustain Maritime/Harbour Security interoperability capability shortfalls fall into the following categories:

• Adaptive information systems:
   o Communications
   o Networks
   o Information Exchange
     ▪ Dynamic Communities of Interest
     ▪ Messaging (CAP, NIEM, EDXL, Other)
• Information Protection Policy Enforcement (Privacy) Services
• Information Security Policy Development/Enforcement;
• Data Aggregation Services
• Tag and label Processing/enforcement Services
• Information Domain Virtualization
• Interagency interoperability Testing
• Training and Exercises
• ... Others | This recommendation addresses elements of the HS observation:1, 2, 9-13, 21, 22, 24, 25
The HS After action reports highlight a general shortfall in SA/DA; which requires the exploitation of exploit digitized information. In a number of areas the foundational technologies and practices are perceived as high risk by stakeholders. The core capabilities have to be simplifies and demystified fro stakeholders.
Excellent example of this form of development and demonstration is the Multi-agency Situational Awareness System (MASAS). MASAS demonstrate the ability to share common alerts across the internet using open standards and commonly available technologies (e.g., Google). MASAS enabled workstations (with extended SA capability) and network connectivity easily be provided at each Centres (emulations) during an exercise. Critical events (alerts) could be provided from a central node during the exercise to reflect the foundation of SA. Demonstrations – providing increased capability in parallel to an exercise (in a progressive manner) will provide stakeholders with the opportunity to assess new capability without large investments and risk.
Tradition system development and deployment practices are too rigid and brittle to address the dynamic real-world requirements of the EM and PS environment where events are typically unpredictable and asymmetric. New practices and technologies are needed to provide higher levels of flexibility and agility; while integrating the capacity to safeguard sensitive information and align to the changing context (participation, roles, responsibilities, escalations, etc.) and dynamics of an incident or event. These new capabilities, services, technologies and standards needed to be developed, demonstrated and deployed. |
| 5 | **Open Standards Development** | Open standards are required:
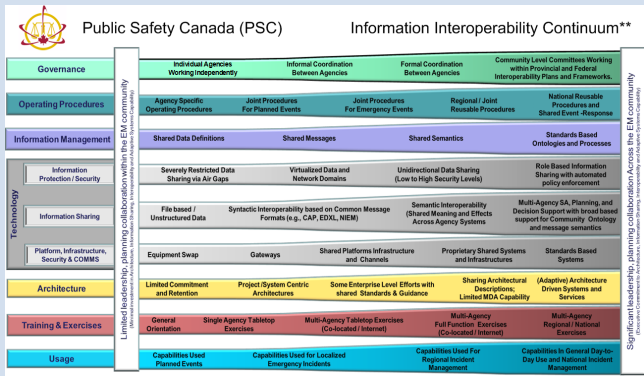
1. Provide a shared set of specifications for the community (versus independently developed specifications);

2. Provide multiple COTS capabilities, services and technologies and | To provide EM and PS community members with the tools needed to develop, deploy, maintain and sustain community interoperability open standards will be required to assure COTS solutions deliver the requisite capabilities. Custom developed systems will be a very expensive option for the many of the partner agencies. Open standards typically deliver multiple |

		vendors to assure competition in the procurement process; 3. Reduce the cost to develop complex procurement specifications and RFPs; and 4. Leverage the knowledge and experience of the broader IM/IT community. The Maritime/Harbour Security community needs to actively influence the development of IM/IT standards that address the nature of their operational environment. There are currently many gaps in the areas of IM/IT and communications standards and technologies in the high risk areas identified above.	vendor options that deliver competitive pricing and solution options. Standards will be required for many of the practices, techniques and capabilities to assure that there are COTS solutions for community members. Interoperable COTS solutions competing will help the community The Canadian S&T community should be influencing and promoting the development of core standards for the EM and PS communities. E.g., participating in the OMG ECMEM, OASIS and NIEM efforts. Collaboration with CSS and TBS would be useful in this area. Due to the stated shortage of resources, the S&T community should provide resource to Canadian industry members already active in these communities to represent Canadian Interests. The S&T community should seek to develop exemplar solutions for the practices, techniques and solutions outlined above. These enhanced capabilities should be demonstrated as part of community exercises to show the benefits of the new capabilities to the community.
6	**Performance Measures and Metrics Aligned to a Conceptual Architecture and Interoperability Continuum**	The documents reviewed during the course of this study identified a need for performance metrics to assess the capabilities of the Maritime/Harbour Security community during inter-agency exercises. A wide variety of metric were offered; they need to be tied to Service Level Agreements, Architecture Elements and the Public Safety Interoperability Continuum to provide consistency across exercises and assessment.	This recommendation addresses elements of the following observations: 1, 2, 14, 15, 25 Performance Measures and metrics should derive form: o **SLAs and MOUs**, which identify the current agreements between agencies and the ability to support existing requirements; o **Architecture elements**, which identifies the community's capabilities in each of the identified architecture elements. These metrics will help the community focus development resources on deficiencies having the greatest cross-section of the community; and where common specifications and/or standards are required. o **Interoperability Continuum** will provide for a common reference for community and self-assessments.
7	**Lessons Learned Registry**	Several participants at the post exercise workshop identified the need to do a better job addressing capability gaps and lessons learned. This comment is mirrored in many meeting and the objectives for the Public Safety EMSIF. The Maritime/Harbour Security community should deploy an information portal where community members share information and ideas about the best strategies and mechanisms to address lessons learned during exercises and operations.	This recommendation addresses elements of HS observation: This recommendation addresses elements of the following observations: 17 One option would be to align this effort with the EMSIF which seeks to develop: o A GC internal site on GCpedia; and o A community site on the DRDC SharePoint Portal. Partnering on this effort may provide a cost effective strategy for the community. **CAUTION**: The registry must be structured in a manner does not assign responsibility for issues to individuals or individual agencies. Most of the challenges faced by the Canadian EM community are near universal – reported by the US, UK, EU and other; however, there are few universally agreed solutions to interoperability exist in practice. In many cases, the challenges will be addressed one at a time, as champions are identified and the collective knowledge and understanding of the community toward the need for interoperable capabilities increases. If the

C.2 Exercises and Training Process Improvement

Ref.	Title	Description	Comments

1	**Repeatable / Managed Process for Planning, executing and Evaluating Interoperability Exercises**	Many of the challenges faced by DRDC during the preparation would be overcome by a standardized process based on the National Exercise Program guide (/training program courses 100-400 levels) and enhanced architecture practices. It is necessary to Too much data capture is required prior to each exercise that s likely reusable or extensible from exercise to exercise:
		
		○ Organizations charts;
		○ SOPs;
		○ MOUs and SLAs;
		○ Community of interest specifications;
		○ Performance Measures and Metrics;
		○ Other.
		
		It is recommended that these practices and procedures be develop in the near term – to enhance the capabilities of the Maritime/Harbour security in the area of "Training and Exercises".
		
			This recommendation addresses elements of the following HS observations: Specifically 16 – but touches of all elements
			Large scale interoperability exercises are complex and difficult to plan, execute and assess. Consistency in planning, execution and assessment over time (recurring training and exercise) is crucial to the development and use of capability and performance metrics, analysis of results and the presentation capability improvement (over the PSC Interoperability Continuum). Some of the areas that could be standardized include:
			
			○ **Documentation:** Standards that identifying the structure, content and format of core artefacts required by planners, participants, evaluators and stakeholders.
			○ **Data Collection**: What data should be gathered during the planning and setup of the exercise (e.g., SOPs, SLAs, systems descriptions, and system configurations). Core set of questions to be posed and measurements gathered during prior to and during the exercises. Care should be taken that data collection does not become intrusive and or skew the results of the exercise.
			○ **Planning & Execution**:
			  ○ **Scripting**: Basic Form, content and granularity of Exercise Scripts (e.g., MSEL);
			  ○ **Modelling:** Basic form, content and granularity of architecture models needed for scenario development and evaluation (which views and viewpoints and required, optional, not needed);
			  ○ **Evaluation Data and Metrics**: Data to be collection during the execution of the event to support assessment and capability development;
			  ○ **Logging**:
			○ **Assessment**: What form of analysis, assessment and review will be conducted pre, during and post exercise. What decisions are expected to result from the exercise and assessment? For the most part the assessment should result in enhancement to the legislative, policy, S&T and development portfolios of the community. Care should be taken to highlight challenges for individual agencies. The overall goal should be the positioning of the community on the continuum and mitigation of risk through the S&T portfolio.
			○ **Reporting**: Specification of reporting tools and dashboards that assist in the consistent presentation of capability and challenges to

planners, participants, evaluators and stakeholders;

o **Self Assessment**: The process should assist participants and stakeholders in a self assessment where targeted challenges are identified; as a basis for their own internal capability portfolio management.

In order for the community to evolve training and exercise practices, it is further recommended that DRDC develop, on behalf of the community:

o **Exercise Domain Model**: describing the information domain for the planning, execution, evaluation and reporting of training and exercise events. The model will describe the information elements to be captured, maintained and reused, and the relationships between those elements.

o **Architecture views**: Based on the TOGAF and DODAF direction of Public Safety Canada (PSC), describe the purpose of the views applicable to the planning, execution, evaluation and reporting phases of an exercise. Identify which of the views and viewpoints are mandatory, optional and not required.

o **Templates**: Descriptions for the format, structure and content of documents, forms and other artefacts generated during the planning, execution, evaluation and reporting phases of an exercise.

The Emergency Management System Interoperability (EMSI) Framework identifies Training and Exercises as Key elements in the evolution of interoperable information systems. Harbour Siren present a good opportunity to evolve and managed/repeatable process for developing, executing and evaluating interoperability exercises across a broad spectrum of EM and PS operations.

Key elements of the of the process:

- Stakeholder expectations are identified
- Stakeholder objectives are commonly understood
- Stakeholders agree the outcomes
- Stakeholders and participants have the ability to self-assess; to identify internal challenges (not reported as part of the community exercise)
- Exercise artefacts are reusable in follow-on training and exercises
- Architecture Models are developed and agreed
- Evaluation Criteria / Metrics are traceable to the architecture models and the PSC interoperability continuum
- There is a clear, reusable set of artefacts from the exercise.

| 2 | **Align Stakeholder Interoperability Expected** | Stakeholder expectations, objectives and outcomes need to be translated into:

o A Maritime/Harbour Security architecture defining the expected outcomes for identified threats and risk;
o Interoperability Policies;
o Service level agreements or Memorandum of Understanding for | This recommendation addresses elements of the following observations: 10.
Stakeholder objectives and expectations should be allocated to a business (conceptual) architecture and aligned to the expected outcomes and associated metrics. This business architecture should include stakeholder expectations for the sharing quality of information |

		Outcomes	sharing of resources across o Event outcome traces o Communities of Interest / Practice o Interagency Processes **(Provided in the HS Process Model)** o Capabilities/services/systems/... o Other ... Much of this information should define the community's priorities and progress on the PSC Interoperability Continuums. The community should initiate: o The development of the aforementioned information; and o Near, Mid, far term targets on the interoperability continuum; and o Transition Plan from current to target capability.	(Accuracy, Relevance, Timeliness, Usability, Completeness, Brevity, Trustworthiness and Protected), the maintenance of situational/Domain Awareness and interagency collaboration.
3		**Exemplar Exercise/Training Model**	The community should develop and exemplar exercise/Training model illustrating the architectural views needed to plan, execute and assess community capability.	This recommendation addresses elements of the following observations: 16. The model should illustrate how exercise planner can simplify models to better communicate with stakeholders and users. Using architecture based approaches will also assist in the validation of consistency between model views. The model should depict each of the required views in sufficient detail to support training of exercise and training planners in the use of architecture. As described earlier, Harbour Siren planning data offers a good start on this Model: 1. Overview and Summary **(Alignment of Current Document)** - **For maritime/harbour security and EMSI** 2. Strategic Capability Transformation (Vision) 3. High Level Operational Concept (including Security / Privacy Concept) 4. Integrated Dictionary **(extension of Current Documentation)** 5. Information Domain Model (Conceptual / Logical)l 6. Operational Resource Flows **(Alignment/Extension of Current Model)** 7. Organizational Relationships **(Alignment/Extension of Current Model)** 8. Operational Activity Decomposition **(Alignment of Current Model)** 9. Operational Rules and performance measures 10. Standards Profile

This page intentionally left blank.

List of symbols/abbreviations/acronyms/initialisms

ADDM	Architecture Domain Meta Model	
AF	Architecture Framework	
AV	All View	
BTEP	Business Transformation Enablement Programme	
C&A	Certification and Accreditation	
CDS	Cross Domain Solutions	
CIOB	Chief Information Officer Branch	
CM	Configuration Management	
CM	Crisis Management	
CoI	Community of Interest	
CoP	Community of Practice	
COP	Common Operating Picture	
CSE	Canadian Security Establishment	
CV	Common View	
CWM	Common Warehouse Model	
DAMA	Data Management Association	
DDL	Data Definition Language	
DEM	Data Exchange Mechanism	
DML	Data Manipulation Language	
DMM	Domain Meta Model	
DNDAF	Department of National Defence Architecture Framework	
DODAF	Department of Defence Architecture Framework	
DTC	Doman Technology Committee	
DTF	Domain Task Force	
EA	Enterprise Architecture	
EM	Emergency Management	
EMSIC	EMSI Catalogue	
EMMS	EMSI Metadata Standards	
EMS	Emergency Management System	
EMPC	EMSI Policy Catalog	
EMSC	EMSI Standards Catalog	
EMSI	Emergency Management System Interoperability	

EMSIF	Emergency Management System Interoperability Framework
EMXL	EMSI XML schema Library
ERD	Entity Relationship Diagram
ERP	Enterprise Resource Planning
ETL	Extract, Transform and Load
FTF	Finalization Task Force
GC	Government of Canada
GC	Governments of Canada
GCFA	GC Federated Architecture
GSRM	Governments Services Reference Model
FAP	Federated Architecture Programme
HV	Human View
IDEAS	International Defence Enterprise Architecture Specification
IEDM	Information Exchange Data Model
IEF	Information Exchange Framework
IER	Information Exchange Requirement
IM	Information Management
JC3IEDM	Joint Consultation, Command and Control Information Exchange Data Model
IS	Information System
ISO	International Standards Organization
ISDM	Information Sharing Domain Model
IT	Information Technology
IV	Information View
KM	Knowledge Management
MEM	Major Event Management
MDA	Model Driven Architecture
MILS	Multi-Independent Levels of Security
MIP	Multilateral Interoperability Programme
MIRD	MIP Information Resource Dictionary
MLS	Multi-Level Security
MODAF	Ministry of Defence Architecture Framework
MOF	Meta Object Facility
MOU	Memorandum of Understanding

NAF	NATO Architecture Framework
NIEM	Nations Information Exchange Model
OASIS	Organization for the Advancement of Structured Information Standards
OCL	Object Constrain language
OGC	Open Geospatial Consortium
OMG	Object Management Group
OV	Operational View
OWL	WEB Ontology Language
PAS	Publically Accepted Specifications
PIP	Platform Independent Model
PSAF	Public Security Architecture Framework
PSBP	Policy, Standards and Best Practices
PS	Public Safety
PSC	Public Safety Canada
PSM	Platform Specific Model
PSSI	Public Safety System Interoperability
PSSI	Public Security System Interoperability
PTC	Platform Technology Committee
PTF	Platform Task Force
QA	Quality Assurance
QoS	Quality of Service
RDF	Resource Description Framework
RDFS	RDF Schema
RTF	Revision Task Force
SA	Situational Awareness
SABSA	*Sherwood Applied Business Security Architecture*
SBVR	*Semantic Business Vocabulary and Rules*
SecV	Security View
SIG	Special Interest Group
SLA	Service Level Agreement
SOA	Service Oriented Architecture
SOP	Standard Operating Procedure
SOPES	Shared Operational Picture Exchange Services
SOS	System of Systems

SQL	Structured Query Language
SV	System View
TB	Treasury Board
TBS	Treasury Board Secretariat
TLAAF	Three Letter Acronym Architecture Framework
TV	Technical View
UML	Unified Modeling Language
UPDM	Unified Profile for DODAF and MODAF
XMI	XML Metadata Interchange
XML	Extensible Mark-up Language
XSD	XML Schema Definition
W3C	World Wide Web Consortium
WG	Working Group

Distribution list

Document No.: DRDC Atlantic CR 2010-179

The distribution list is not included in the report.

This page intentionally left blank.

DOCUMENT CONTROL DATA		
(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)		

| 1. | ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

Advanced Systems Management Group Ltd
265 Carling Ave, Suite 630
Ottawa, ON
K1T 4G3 | 2. | SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED
(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC JUNE 2010 |

3.	TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.) Harbour Siren: Technical Recommendations Report

4.	AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used) Abramson, M.

5.	DATE OF PUBLICATION (Month and year of publication of document.) September 2010	6a.	NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.) 74	6b.	NO. OF REFS (Total cited in document.) 11

7.	DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.) Contract Report

8.	SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.) Defence R&D Canada – Atlantic 9 Grove Street P.O. Box 1012 Dartmouth, Nova Scotia B2Y 3Z7

9a.	PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.) 33cl	9b.	CONTRACT NO. (If appropriate, the applicable number under which the document was written.) EN578-060502/006/ZT

10a.	ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b.	OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.) DRDC Atlantic CR 2010-179

11.	DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.) Unlimited

12.	DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.)) Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This study was commissioned by Defence Research and Development Canada – Atlantic (DRDC Atlantic) as part of a project on Harbour Security that was funded by the Marine Security Coordination Fund of the Interdepartmental Marine Security Working Group (IMSWG). The document outlines a series of observations and technical recommendations resulting from a post Harbour Siren 2009 document review conducted by Advanced Systems Management Group Ltd. The review looked at the information, practices, standards, tools used during planning, execution and assessment of the Harbour Siren exercise, with the objective of the review being a set of recommendations and a near term road map for Emergency Management Interoperability (EMI) and Emergency Management System Interoperability (EMSI). The analysis provided recommendations related to: 1) the EMSI Capability Portfolio, focusing on the development/deployment voice and data interoperability capability; and 2) on Exercise Process Improvement, focusing on improving exercise planning, executions and assessment. The recommendations build on the Harbour Siren observations and provide strategies for the community to develop greater capability, flexibility, agility and adaptability in their ability to interoperate. Key areas include: A) shared community vision for voice and data communication; B) shared community understanding of requirements resulting from this shared vision; C) provision of shared situational/domain awareness; and D) enhancement of interagency collaboration.

Cette étude a été commandée par Recherche et développement pour la défense Canada – Atlantique (RDDC Atlantique) dans le cadre d'un projet concernant la sécurité portuaire financé par le Fonds de coordination de la sûreté maritime du Groupe de travail interministériel sur la sûreté maritime (GTISM). Le document présente un ensemble d'observations et de recommandations techniques résultant d'un examen de documents connexes à l'exercice *Harbour Siren* 2009, qui a été effectué par *Advanced Systems Management Group Ltd*. L'examen a porté sur l'information, les pratiques, les normes et les outils utilisés durant la planification, l'exécution et l'évaluation de l'exercice *Harbour Siren*, dans le but de dégager un ensemble de recommandations et une feuille de route à court terme pour l'interopérabilité dans la gestion des urgences (IGU) et l'interopérabilité du système de gestion des urgences (ISGU). Cette analyse a permis de dégager des recommandations relativement : 1) au portefeuille de capacités de l'ISGU, axé sur le développement et la mise en œuvre d'une capacité d'interopérabilité voix-données; 2) à l'amélioration du processus des exercices, axée sur l'amélioration de la planification, de l'exécution et de l'évaluation des exercices. Les recommandations sont basées sur l'observation de l'exercice *Harbour Siren,* et elles fournissent à la communauté des stratégies pour développer une plus grande capacité, flexibilité, souplesse et adaptabilité en matière d'interopérabilité. Elles portent essentiellement sur les points suivants : A) perception commune, au sein de la communauté, pour les transmissions vocales et de données; B) compréhension commune des exigences découlant de cette perception; C) développement d'une connaissance commune de la situation/du domaine; D) renforcement de la collaboration interorganismes.

This page intentionally left blank.

Defence R&D Canada

Canada's leader in defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

DEFENCE **R&D** DÉFENSE

www.drdc-rddc.gc.ca